e-crime & cybersecurity FRANCE VR

30 juin 2020
Online

@eCrime_Congress
#ecrimecongress

#ecrimecongress

Sécuriser le télétravail
Se protéger des nouvelles cyber menaces, maintenir la continuité des activités, soutenir le passage au numérique

AMI OU ENNEMI?

De nos jours, les cyberattaquants sont des maîtres de l'illusion

Attaques sophistiquées par email, système cloud compromis, appareils vulnérables - il est difficile de prédire les menaces de demain. L'IA fait la distinction entre une activité légitime et une cybermenace émergente, et riposte en quelques secondes.

Faites un essai de 30 jours et rejoignez les milliers d'organisations protégées par la Cyber AI de Darktrace.

darktrace.fr

DARKTRACE
Leader Mondial de la Cyber IA

Jusqu'en mars 2020, la grande nouveauté en matière de cybersécurité en France était les récentes sanctions de la CNIL sur, par exemple, SERGIC et Active Assurances (au titre de l'article 32 du RGPD), des sanctions déclenchées par des manquements fondamentaux à la mise en œuvre de mesures de sécurité appropriées pour assurer la sécurité des données clients. Les exigences de divulgation et les sanctions du RGPD ont indiqué que lors de la numérisation de leurs entreprises, celles-ci avaient et ont encore du mal à sécuriser leurs données de base.

Puis vint la crise du COVID-19 et le verrouillage, forçant des effectifs entiers à opérer depuis leur domicile et les entreprises de tous secteurs déplaçant l'engagement des clients vers le domaine numérique. Par nécessité, l'accès à distance et des privilèges étendus ont été accordés à travers les organisations. Tout comme les entreprises étaient au point de perturbation maximale, les équipes de cybersécurité faisaient également face à une énorme augmentation des volumes et de la gravité des menaces. Le phishing, les attaques DDoS et les ransomwares ont tous connu une forte augmentation dans cet environnement. Des collaborateurs qui utilisent des systèmes inconnus ou non sécurisés sont plus faciles à pirater et une perturbation globale des activités rend probablement les contrôles compensatoires moins efficaces.

Et maintenant, la France prévoit de sortir de son état d'urgence sanitaire contre les coronavirus à partir du 10 juillet, avec une proposition de loi qui inclura une période de transition pendant laquelle le pays pourrait réimposer des restrictions de mouvement. Le conseil scientifique du gouvernement propose une période de quatre mois pendant laquelle le Premier ministre pourrait restreindre les mouvements pour contrôler l'épidémie en dernier recours.

Alors qu'est-ce que cela signifie pour les lieux de travail, les entreprises et la cybersécurité ? Quel ratio de télétravail restera au sein des entreprises pour les collaborateurs ? La numérisation accélérée déclenchée par le COVID-19 est-elle temporaire ou permanente? Les entreprises ont-elles réalisé que la résilience provient du SaaS et du Cloud ? Quels problèmes informatiques et de cybersécurité sont créés par ces tendances et par un retour partiel au travail ?

Nous sommes ravis de mettre en ligne le 9e Congrès e-Crime & Cybersécurité France ! En l'absence de réunions physiques, l'événement est une opportunité fantastique d'écouter et participer à des études de cas réels et des séances techniques approfondies de pairs qui naviguent également dans la cybersécurité par contrôle à distance. L'un des objectifs continus de nos événements est de faciliter la conversation, alors profitez-en pour vous créer des opportunités de networking avec vos confrères et consoeurs dans le salon virtuel prévu à cet effet, poser des questions aux intervenant(e)s de l'auditorium et visiter le hall d'exposition pour vous mêler aux fournisseurs de solutions. Nous espérons que vous apprécierez l'événement, n'hésitez pas à contacter notre équipe au bureau d'inscription virtuel si vous avez des questions !

Ruby Mercer | Editrice

@eCrime_Congress **#ecrimecongress**

30 juin 2020

Onlines

Editor:
Ruby Mercer
e: ruby.mercer@akjassociates.com

Design and Production:
Julie Foster
e: julie@fosterhough.co.uk

Forum organiser:
AKJ Associates Ltd
27 John Street
London WC1N 2BX
t: +44 (0) 20 7242 4364
e: ruby.mercer@akjassociates.com

© AKJ Associates Ltd 2020. Tous droits reservés. La reproduction d'une partie ou de l'ensemble sans autorisation écrite est strictement interdite.

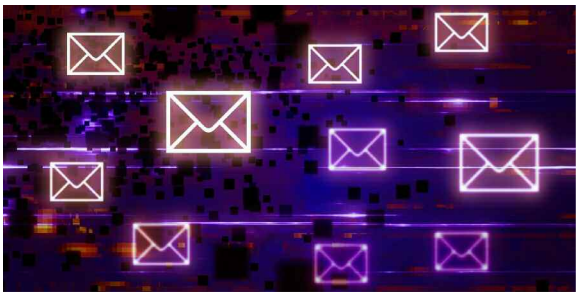
Les articles publiées dans le magazine ne reflètent pas nécessairement les opinions d'AKJ Associates Ltd. Les rédacteurs en chef et les auteurs de ce magazine n'engagent pas leur responsabilité pour les erreurs contenues dans la publication, ou pour toutes omissions. Ce magazine ne prétend pas offrir d'investissement, de conseil juridique ou d'autre type de conseil et ne devrait pas être lu dans ce sens.

Les organisations sponsorisant ou soutenant e-Crime & Cybersecurity France VR n'encourent aucune responsabilité, singulièrement ou collectivement, pour le contenu de ce magazine. Aucune de ces organisations sponsorisant ou soutenant e-Crime & Cybersecurity France VR ne peut, singulièrement ou collectivement, prendre la responsabilité de l'utilisation du contenu qui peut être rendue à l'intérieur de ce magazine.

The domain game: how email attackers are buying their way into inboxes

De nombreux outils de sécurité e-mails ont du mal à détecter les menaces qu'ils rencontrent pour la première fois.

Par Dan Fein



Il est désormais de notoriété publique que la grande majorité des cybermenaces commencent par un e-mail. Dans les conditions de travail actuelles, cela est plus vrai que jamais : Une étude récente fait état d'une augmentation de 30 000% du phishing, des sites Web et des logiciels malveillants ciblant les utilisateurs travaillant à distance.

De nombreux outils de sécurité e-mails ont du mal à détecter les menaces qu'ils rencontrent pour la première fois. Les attaquants le savent et utilisent de nombreuses techniques pour tirer parti de cette faille fondamentale. Cela inclut l'automatisation pour muter les variantes de menaces courantes, entraînant une augmentation massive des menaces inconnues. Une autre technique, qui sera au centre de cet article, est la création rapide et généralisée de nouveaux domaines afin d'éviter les contrôles de réputation et la détection basée sur les signatures.

La récente émergence exponentielle de création de domaines

Alors que les outils traditionnels doivent s'appuyer sur l'identification des campagnes et des modèles sur plusieurs e-mails pour déterminer si un e-mail est malveillant ou non, la technologie Cyber IA de Darktrace ne nécessite pas de classer les e-mails en compartiments pour savoir si ils sont ou non légitimes. Il n'est donc pas nécessaire de suivre activement les campagnes. Cependant, en tant que chercheurs en sécurité, il est difficile de passer à côté de certaines tendances.

Depuis l'épidémie de Coronavirus, nous avons observé l'enregistrement de plus de 130 000 domaines liés au Covid-19. Au cours de cette période, 60% des menaces de spear phishing neutralisées par Antigena Email étaient liées au Covid-19 ou au télétravail. Une autre étude récente a déterminé que 10 000 domaines liés aux coronavirus sont créés chaque jour, dont environ neuf sur dix sont malveillants ou tentent de générer des ventes de faux produits.

Les attaquants profitant également de la modification des comportements en ligne résultant de la pandémie, une autre tendance que nous avons constatée est la prolifération du mot-clé « Zoom » dans certains des domaines impopulaires qui ont contourné les outils traditionnels, car les attaquants exploitent la récente montée en puissance de la plate-forme de visioconférence.

« Je pense que les pirates informatiques ont identifié le Coronavirus comme étant une source de questionnement et de recherche d'informations par les utilisateurs. La panique mène à une pensée irrationnelle et les gens en oublient les bases de la cybersécurité. » COO, Atlas VPN

J'ai récemment écrit un article de blog sur l'idée du « Fearware » et sur la raison de son succès. À l'heure actuelle, les gens recherchent désespérément des informations, et les attaquants le savent. Les cybercriminels jouent sur la peur, l'incertitude et le doute à travers un certain nombre de mécanismes, et nous avons observé une grande variété de tentatives très créatives pour impliquer les destinataires. Ces e-mails vont des faux « traqueurs de virus » à l'envoi d'e-mails censés provenir d'Amazon, proclamant une augmentation ingérable des nouveaux comptes enregistrés et exigeant une « réinscription » des coordonnées de la carte de crédit du destinataire s'il souhaite conserver son compte.

Achat de nom de domaine: Un cercle vicieux

L'achat de milliers de nouveaux domaines et l'envoi de courriels malveillants en masse est une technique éprouvée que les cybercriminels utilisent depuis des décennies. De nos jours, grâce à l'automatisation, ils le font plus rapidement que jamais.

Voici pourquoi cela fonctionne.

Les outils de sécurité traditionnels fonctionnent en analysant les e-mails de manière isolée, en les

comparant à des listes noires statiques de « problèmes connus ». Par analogie, l'outil de passerelle agit ici comme un gardien de sécurité se tenant au périmètre des locaux physiques d'une organisation, demandant à chaque individu qui entre : « êtes-vous malveillant ? »

La réponse binaire à cette seule question est extraite en consultant certaines métadonnées autour de l'e-mail, y compris l'adresse IP de l'expéditeur, son domaine d'adresse e-mail et tous les liens ou pièces jointes intégrés. Ils analysent ces données dans le vide et s'intéressent uniquement à leur valeur nominale, sans tenir compte de la relation entre ces données, le destinataire et le reste de l'entreprise. Ils effectuent des vérifications de réputation, demandant « Ai-je déjà observé cette IP ou ce domaine? » Évidemment, lorsque la réponse est non, ils les laissent passer car ce ne sont pas des menaces identifiées au préalable.

Lorsque le domaine vient tout juste d'être crée, il n'a pas encore de réputation. Ces outils traditionnels ayant une capacité limitée à identifier les éléments potentiellement nuisibles par tout autre moyen, ils n'ont pas d'autre choix que de les laisser entrer par défaut.

Ces méthodes effleurent à peine la surface d'un éventail beaucoup plus large de caractéristiques qu'un e-mail malveillant peut contenir. Les menaces par courrier électronique devenant de plus en plus sophistiquées, l'approche « présomption d'innocence jusqu'à preuve du contraire » ne suffit pas. Pour une vérification complète, il faudrait questionner :

- Le domaine a-t-il déjà eu une relation avec le destinataire? L'organisation dans son ensemble?
- Est-ce que cela ressemble étrangement visuellement à d'autres domaines?
- Est-ce la première fois que nous voyons un e-mail entrant de cet utilisateur?
- Quelqu'un dans l'organisation a-t-il déjà partagé un lien avec ce domaine?
- Un utilisateur a-t-il déjà visité ce lien?

Les outils existants posent ouvertement les mauvaises questions, auxquelles les attaquants connaissent les réponses. Et généralement, ils peuvent contourner ces sécurités inattentives en ne payant que quelques centimes pour de nouveaux domaines.

Comment se frayer un chemin

Prenons le point de vue d'un attaquant. Un simple e-mail peut suffire à pénétrer un réseau, et peut parfois même constituer la clé du royaume. Un achat initial de quelques milliers de nouveaux domaines sera donc presque inévitablement payant. Tant que cela fonctionne et qu'ils en profitent, le jeu en vaut donc la chandelle.

C'est exactement ce que font les attaquants. Les domaines nouvellement enregistrés passent systématiquement par des passerelles jusqu'à ce que les outils traditionnels soient armés avec suffisamment d'informations pour déterminer que ces domaines sont mauvais, date à laquelle des milliers voire des millions d'e-mails ont pu être distribués avec succès. Dès que l'infrastructure d'attaque est épuisée, les attaquants l'abandonnent et achètent et déploient très facilement un nouvel ensemble de domaines.

Ainsi, le cercle vicieux continue. Les solutions traditionnelles continueront à intercepter uniquement les mauvais e-mails reconnus – Pendant ce temps, des milliers de domaines malveillants sont préparés en vue de la prochaine campagne. C'est le « Domain Game », et c'est un jeu extrêmement difficile à gagner pour les défenseurs.

Poser les bonnes questions

Heureusement, la solution à ce problème est aussi simple que le problème lui-même. Cela nécessite de s'éloigner de l'ancienne approche et de déployer une technologie à la hauteur de la vitesse et de l'ampleur des attaquants d'aujourd'hui.

Au cours des deux dernières années, de nouvelles technologies exploitant l'IA ont émergé, cherchant à comprendre l'humain derrière l'adresse e-mail. Plutôt que d'inspecter le trafic entrant au niveau de la surface et de poser des questions binaires, ce changement de paradigme face à l'approche traditionnelle permet de poser les bonnes questions: non seulement « êtes-vous malveillant ? », Mais surtout: « êtes-vous légitimes et partie intégrante ? »

Grâce à une compréhension nuancée du destinataire, de ses pairs et de l'organisation dans son ensemble, chaque e-mail entrant, sortant et interne est analysé dans son contexte, puis ré-analysé à maintes reprises à la lumière des preuves en constante évolution. Poser les bonnes questions et comprendre l'humain établit invariablement une norme beaucoup plus élevée pour des taux de capture acceptables avec des menaces inconnues lors de la première rencontre. Cette approche dépasse de loin les défenses de messagerie traditionnelles qui se sont avérées défaillantes et rendent les entreprises et leurs employés vulnérables aux e-mails malveillants dans leur boîte de réception.

Plutôt que de dénigrer désespérément les domaines et les adresses IP sur liste noire dans une tentative malheureuse de battre les attaquants, nous pouvons changer complètement le jeu, faire pencher la balance en faveur des défenseurs afin de sécuriser nos boîtes de réception et nos organisations dans leur ensemble. □

En savoir plus sur Antigena Email.

Dan Fein, Directeur Amériques des Produits de Sécurité E-mail, Darktrace

Pour plus d'informations :
www.darktrace.com

SentinelOne Singularity la plate-forme qui déjoue toutes les attaques 365 jours par an

Cette première plate-forme XDR, optimisée par l'IA, révolutionne la sécurité de l'entreprise.

Par SentinelOne

SentinelOne est le premier éditeur à avoir fait évoluer une solution autonome de protection des endpoints gérés dans le cloud en une plateforme de cybersécurité complète, bénéficiant de la même base de code unique et d'un modèle de déploiement simple. Il est aussi le premier à avoir intégré dans une plateforme XDR la protection des objets connectés et des cloud workload. Facile à administrer, Singularity permet de prévenir, détecter, traquer et répondre aux menaces sur tous les actifs de l'entreprise lui donnant la possibilité de déceler ce qui n'a jamais été vu auparavant et de maîtriser l'inconnu.

Protection des postes de travail (EPP)

La solution EPP de SentinelOne assure une prévention des attaques sur tous les principaux vecteurs, une élimination rapide des menaces grâce à des capacités de réponse entièrement automatisées et régies par des règles ainsi qu'une visibilité complète sur l'environnement des postes de travail grâce à des analyses contextualisées et en temps réel. En tant que pionnier de l'IA comportementale, SentinelOne propose de nombreux algorithmes d'IA brevetés qui assurent une protection – et même une remédiation automatique – contre le plus large éventail de menaces qui soit, sans être tributaire de la bande passante, de la latence du cloud ni de l'intervention humaine.

Détection et riposte (EDR)

Au-delà des solutions antivirus et EDR traditionnelles et de nouvelle génération, ActiveEDR de SentinelOne permet aux équipes de sécurité de comprendre rapidement le scénario d'attaque et son origine, et d'y répondre de manière autonome. Le module Deep Visibility Threat Hunting offre une approche contextuelle rapide, pré-indexée et riche permettant de traquer les menaces sur l'ensemble du trafic, crypté ou non. Les analystes n'ont plus à parcourir les arborescences de processus, et à passer des heures à comprendre ce qui se passe. Avec ActiveEDR, chacun, de l'analyste SOC chevronné au néophyte de l'équipe de sécurité, peut automatiquement remédier aux menaces et se défendre contre des attaques avancées.

Découverte et contrôle pour l'Internet des objets (IoT)

La solution Ranger renforce les dispositifs protégés par SentinelOne avec des capacités de découverte et de segmentation de l'IoT. Ranger détecte non seulement les dispositifs intelligents et appareils non référencés, mais procède également à leur segmentation. Toutes les données IoT sont directement intégrées à Singularity pour faciliter la détection des menaces et proposer un contexte inédit. En utilisant l'IA pour surveiller et contrôler l'accès à chaque dispositif IoT, SentinelOne permet aux machines de résoudre un problème jusqu'ici impossible à gérer à grande échelle.

La solution EPP de SentinelOne assure une prévention des attaques sur tous les principaux vecteurs, une élimination rapide des menaces grâce à des capacités de réponse entièrement automatisées et régies par des règles ainsi qu'une visibilité complète sur l'environnement des postes de travail grâce à des analyses contextualisées et en temps réel.

Protection des conteneurs et des workloads

La protection des conteneurs et des cloud workload s'appuie sur les capacités de réponse autonomes et l'IA comportementale de SentinelOne sur les principales plates-formes Linux, physiques et virtuelles, les cloud workload et les conteneurs Kubernetes, assurant ainsi la prévention, la détection et la réponse aux cybermenaces actuelles et de demain. Cela comprend les fichiers malveillants et les attaques dynamiques dans les environnements cloud natifs et conteneurisés, offrant des options de réponse avancées et une remédiation autonome. □

Pour plus d'informations :
www.sentinelone.com

SentinelOne™

BREACHES Stop HERE

NOUS SOMMES EN MISSION DE STOPPER TOUTE BRÈCHE ET TOUTE ATTAQUE POTENTIELLE

Notre technologie est basée sur un unique agent, ultra-light, allié à la puissance du cloud.

Nous vous offrons:

1. Détection de la menace en moins d'une minute
2. Identification de la menace en moins de 10 minutes
3. Éradication de la menace en moins de 60 minutes

Pour profiter d'une évaluation gratuite, visitez:

www.crowdstrike.fr

La baguette magique n'opère que si le magicien a du talent

Tirer le meilleur parti des outils de prévention.

Par Thomas Etheridge

28 mai 2020,
From The Front Lines

À l'heure où les entreprises sont confrontées aux réalités du passage au télétravail et à une conjoncture économique incertaine, la prévention est plus importante que jamais. Les cyberpirates cherchent à tirer parti du climat actuel et des failles de sécurité. L'équipe des Services CrowdStrike® constate en effet un nombre sans précédent d'infections par ransomware, de fuites de données et d'attaques ciblées. Elle a également observé une tendance inquiétante : la plupart des entreprises n'exploitent pas les fonctionnalités de prévention conçues pour bloquer les activités malveillantes.

L'incapacité à configurer correctement ces outils fait souvent plus de tort que leur absence, car ils donnent à l'entreprise un faux sentiment de sécurité, sans compter l'argent gaspillé. Même si le phénomène n'est pas nouveau, la multiplication des ransomwares et d'autres attaques perturbatrices aggrave la situation pour les entreprises qui ne parviennent pas à bloquer efficacement les activités malveillantes.

Des outils de sécurité mal configurés

Il n'est pas rare que l'équipe des Services CrowdStrike tombe sur des outils de sécurité de pointe mal déployés ou mal gérés. Les problèmes rencontrés sont divers : vulnérabilités non corrigées (qui laissent passer les exploits), graves erreurs de configuration, déploiements bâclés ou paramètres de prévention inadéquats permettant aux cyberpirates d'infecter les endpoints pour ensuite se déplacer latéralement dans tout l'environnement. Les grandes entreprises ne sont pas épargnées : au contraire, l'équipe des Services CrowdStrike a constaté qu'elles sont plus susceptibles de ne pas configurer leurs outils de sécurité ou de commettre des erreurs lorsqu'elles le font. Certes, les grandes entreprises ont nettement plus de ressources que les petites structures. Pour autant, elles doivent souvent gérer un environnement en expansion, des réseaux complexes et plusieurs projets d'amélioration de front, sans toujours parvenir à finaliser les détails. Et malheureusement, il est fort probable que la transition vers le télétravail – caractérisé par un environnement et un modèle de fonctionnement encore plus distribués et à distance – aggrave le problème.

Les plateformes de détection des menaces sur endpoints ne sont pas les seules concernées. L'équipe des Services CrowdStrike a également identifié des erreurs de configuration critiques dans les systèmes de prévention des intrusions, les outils de prévention des fuites de données, les plateformes d'authentification à plusieurs facteurs et les solutions CASB (Cloud Access Security Broker). Par exemple, lors de certaines missions d'intervention sur incident, elle a remarqué que, malgré la mise en place de contrôles de sécurité (tels que des pare-feux de nouvelle génération avec segmentation des réseaux d'entreprise et de production), les victimes n'avaient pas configuré les règles de pare-feu. Résultat : des malwares se sont rapidement propagés latéralement pour infiltrer les équipements de production stratégiques.

La nécessité de renforcer les capacités de prévention

Les erreurs de configuration ne sont probablement pas plus fréquentes aujourd'hui qu'il y a quelques années. Cela dit, les tendances actuelles en matière de menaces font que la prévention joue un rôle plus déterminant et que, de ce fait, le problème posé par les outils mal configurés ou insuffisamment optimisés a pris de l'ampleur. Et il se manifeste de plusieurs façons, comme dans la plupart des situations où le facteur humain intervient dans la cybersécurité. Dans certains cas, les outils de sécurité sont déployés en mode « surveillance » ou « détection » lors des tests de preuve de concept (POC) afin d'éviter toute perturbation au sein de l'environnement, et les fonctionnalités de prévention plus strictes ne sont jamais activées.

Dans d'autres cas, l'équipe de sécurité informatique demande l'activation de ces fonctionnalités, mais l'équipe informatique n'en tient pas compte, soit parce qu'elle ne fait pas confiance à l'outil en question, soit parce que ses priorités sont ailleurs. Plus troublant encore, certaines entreprises achètent des outils de sécurité dans le seul but de se mettre en règle avec les obligations de conformité et ne les implémentent jamais complètement, de sorte que les équipes de cybersécurité croient à tort qu'une protection est en place.

Il n'y a pas de cause unique au problème, et donc pas de solution miracle. Néanmoins, les entreprises peuvent prendre certaines mesures pour optimiser l'efficacité de leurs outils, tant dans l'immédiat que dans une optique à long terme, afin d'instaurer les bonnes pratiques :

- *Ne jamais acheter un outil purement à des fins de conformité.* S'il est tout à fait concevable que la conformité motive un achat technologique, des

Les tendances actuelles en matière de menaces font que la prévention joue un rôle plus déterminant et que, de ce fait, le problème posé par les outils mal configurés ou insuffisamment optimisés a pris de l'ampleur.

personnes doivent être chargées d'utiliser et d'optimiser les outils et processus connexes.

- *Développer des plans d'implémentation pour tous les nouveaux outils.* Ces plans doivent faire intervenir les équipes informatique et de sécurité informatique de façon à garantir que les parties prenantes soient informées de la fonction et de l'usage prévu de chaque outil. Lors de cette planification, il faut également établir l'impact opérationnel de l'outil sur les activités et le degré de tolérance d'un tel impact.
- *Définir une fréquence régulière d'examen des outils de sécurité.* Comme ces solutions sont souvent régulièrement enrichies de nouvelles fonctionnalités, votre équipe doit évaluer, tester et implémenter des plans de déploiement à mesure que celles-ci sont disponibles sur le marché. Un déploiement initial sans aucun suivi tourne inévitablement au fiasco, car les menaces ainsi que les tactiques et techniques d'attaque évoluent plus rapidement que la plupart des outils.
- *Fixer des règles en matière de gestion des changements.* La configuration approuvée d'un outil doit être documentée et vérifiée plusieurs fois par an. L'équipe de sécurité informatique doit fréquemment aborder la question des configurations et des nouvelles fonctionnalités avec les fournisseurs et l'équipe de support afin de tirer le meilleur parti de l'outil et de s'assurer qu'il est utilisé de façon correcte dans l'environnement de l'entreprise.
- *Développer un cadre de détection et de prévention.* Les outils ne doivent pas tous être déployés en activant les configurations de prévention les plus rigoureuses, surtout lorsque des mesures compensatoires sont en place. La mise en œuvre d'un cadre de détection et de prévention doit permettre d'identifier les menaces que l'entreprise veut bloquer, les cas d'utilisation qu'elle souhaite prendre en charge, de même que les outils correspondant à chaque cas. En plus de constituer une excellente base pour déterminer les scénarios liés à la prévention et ceux associés à la détection, ainsi que les outils nécessaires dans les deux cas, ce cadre représente une source importante d'indicateurs de performance de la sécurité.
- *Tester le fonctionnement de ses outils.* Il est important de réaliser régulièrement des audits et des exercices de simulation d'attaque pour vérifier que les outils déployés fonctionnent comme prévu.
- *Déterminer les risques prioritaires.* Idéalement, les entreprises devraient constamment optimiser leurs outils, en se fixant comme objectif une sécurité sans faille. Mais cela suppose d'en avoir le temps et les ressources, ce qui n'est pas le cas de la plupart des entreprises. S'il vous est impossible de tout cadenasser, établissez votre plan de bataille. Identifiez les types d'attaques à bloquer en priorité et concentrez-vous sur celles-ci.

Consultez le Centre de ressources Cybersécurité et COVID-19 de CrowdStrike pour obtenir des conseils afin de protéger au mieux votre entreprise durant cette période sans précédent. Téléchargez également le Rapport des Services CrowdStrike sur leur expérience aux avant-postes de la cybersécurité pour découvrir les observations faites par nos experts sur le terrain en 2019 et les principales tendances de l'année 2020. □

Autres ressources :
Regardez notre webcast à la demande Regardez notre webcast à la demande CrowdStrike Cyber Front Lines Report CrowdCast qui analyse de façon approfondie les observations, les tendances et les thèmes abordés dans le rapport.

Lisez la présentation du rapport rédigée par Shawn Henry, Directeur de la sécurité et président des Services CrowdStrike.

Consultez cette page web pour en savoir plus sur l'équipe des Services CrowdStrike et la manière dont elle peut aider votre entreprise à renforcer sa cybersécurité.

Apprenez-en davantage sur la plateforme CrowdStrike Falcon et ses avantages.

Essayez par vous-même notre antivirus de nouvelle génération. Commencez sans plus tarder votre évaluation de Falcon Prevent™.

Pour plus d'informations :
www.crowdstrike.com

CROWDSTRIKE

Hacking éthique : Quatre idées reçues sur les plateformes de bug bounty

Il est difficile aujourd'hui de démêler le vrai du faux au sujet des plateformes de bug bounty.

Par Hugues Masselin

Face à l'émergence et au développement rapide de ces plateformes de sécurité collaborative, les idées préconçues se sont multipliées. Le hacking éthique offre aux entreprises la possibilité de renforcer leurs systèmes de défense ainsi que de limiter au maximum toutes vulnérabilités. Mais pour certains, le hacking éthique reste un domaine peu connu, voire méconnu.

Qu'est-ce qu'une plateforme de bug bounty ? Comment les entreprises peuvent-elles en tirer profit afin d'améliorer leur cyberdéfense? Afin de pouvoir mieux appréhender le hacking éthique et les plateformes de bug bounty, il est intéressant d'identifier les quatre principales idées reçues sur le sujet dans le but de les démystifier, d'informer et de partager les meilleures pratiques.

Mythe n°1 : les programmes de bug bounty doivent être publics

Les plateformes de bug bounty permettent aux organisations de challenger la qualité et la sécurité de leurs solutions via un programme de sécurité sponsorisé. Ces programmes permettent de garantir la participation de hackers éthiques professionnels et de bénéficier d'une surveillance 24/24 et 7/7, dans le but de détecter toute vulnérabilité qui aurait pu passer inaperçue. Les hackers motivés et créatifs sortent souvent des sentiers battus. Ils interviennent de manière intelligente et contribuent à améliorer les stratégies de cybersécurité en vigueur.

Les programmes publics de bug bounty (les VDP : Vulnerability Disclosure Program) sont un moyen de prouver publiquement le degré de sécurité des solutions proposées par une organisation. *"Si vous pensez que notre service n'est pas sûr, nous vous mettons au défi de trouver un bug !"* Il n'est pas nécessaire cependant que tous les programmes soient publics. En réalité, la plupart des programmes de bug bounty s'avèrent être privés.

Afin de pouvoir mieux appréhender le hacking éthique et les plateformes de bug bounty, il est intéressant d'identifier les quatre principales idées reçues sur le sujet dans le but de les démystifier, d'informer et de partager les meilleures pratiques.

Au sein d'un programme privé, un comité réduit de hackers est invité à rechercher des failles. Les critères de sélection sont généralement basés sur l'expérience, les compétences, l'emplacement et la disponibilité. Chaque rapport, chaque participant, chaque récompense de bug bounty, chaque aspect du programme reste entièrement privé. La plupart des organisations commencent par adopter un programme privé, puis en parlent publiquement une fois le processus de gestion des vulnérabilités bien assimilé, le budget des primes établi, les équipes juridiques et marketing informées, et après avoir simplifié les communications DevSecOps.

Les entreprises ne doivent pas hésiter à communiquer ouvertement au sujet du hacking éthique, car elles peuvent en retirer de nombreux avantages. Les entreprises qui s'expriment librement sur le sujet de la sécurité sont perçues comme ouvertes et transparentes. Cette approche leur permet de montrer qu'elles se soucient des données de leurs clients et qu'elles font tout ce qui est en leur pouvoir pour remédier aux vulnérabilités. Enfin sans aucun doute, l'un des principaux avantages d'en parler publiquement et d'accroître les contributions est d'attirer les meilleurs talents. Les bug bounty rendus publics démontrent que la sécurité est prise au sérieux et qu'elle doit être une priorité.

Mythe n°2 : les bug bounty doivent être menés à longueur d'année

Si certaines organisations choisissent d'exécuter des programmes de bug bounty en continu, beaucoup optent également pour des challenges limités dans le temps. Ces types de programmes impliquent des tests sur un périmètre défini, souvent en utilisant un nombre déterminé de hackers avec un engagement à court terme.

Les programmes de bug bounty sont personnalisables. Il est facile de calibrer un programme de bug bounty privé de manière à ce que le nombre de rapports reçus n'excède pas la capacité de traitement. Il est également possible de gérer le budget et le temps imparti. Cela permet aux entreprises de savoir quand les tests sont déployés et de préparer les équipes informatiques.

Cette approche offre un excellent moyen de découvrir les prémisses du hacking éthique, car une fois les équipes de sécurité engagées, l'entreprise peut tendre

Tandis que “le logiciel dévore le monde” et que l’interconnexion des systèmes devient la norme, penser qu’il est possible de sécuriser ses systèmes en interne s’apparente à une vision dépassée de la sécurité.

vers un engagement continu. Ce type de stratégie permet également aux petites organisations ayant des équipes informatiques réduites de tirer profit du hacking éthique, dans la mesure où elles seront capables d’anticiper des rapports de vulnérabilité. Tout le monde, start-up à multinationale peut bénéficier d’une sécurité renforcée par des hackers éthiques.

Mythe n°3 : Vous devez accorder des primes pour travailler avec des hackers professionnels

Cela va fortement dépendre du programme que vous souhaitez mettre en œuvre. Un programme de divulgation des vulnérabilités (VDP) est un moyen d’avoir un retour sur les vulnérabilités, sans la contrepartie d’une récompense financière. Similaire à un numéro d’urgence sur Internet, ce type de programme met à disposition un canal pour signaler et recevoir les urgences numériques.

L’objectif premier d’un VDP est de recevoir gratuitement des rapports de vulnérabilités provenant de chercheurs en sécurité, externes à l’entreprise. Les entreprises peuvent ainsi éviter quelques surprises comme la divulgation d’une vulnérabilité sur Twitter ou via le service client. Nombreux sont les gouvernements et entreprises qui hébergent une plateforme de VDP car elle leur permet d’instaurer un dialogue avec le public et d’améliorer leur sécurité. Après tout, aucun citoyen n’aimerait que ses données soient exposées, et les hackers éthiques auront souvent tendance à valoriser leurs compétences tout en venant en aide aux organisations publiques.

Il existe d’autre part un marché concurrentiel de bug bounty, en raison de l’incitation financière qui y est corrélée. La prime moyenne versée est de 800 $, il arrive cependant qu’elles soient inférieures à ce montant. D’autres sont beaucoup plus élevées, pouvant aller jusqu’à 1 000 000 $. Le montant dépend souvent des compétences et des efforts requis pour détecter le bug.

Mythe n°4 : Le bug bounty n’encourage pas les développeurs à communiquer avec les hackers

Chaque bug corrigé rend la vie numérique plus sûre, et ce sont les développeurs qui réalisent cette tâche essentielle. Les développeurs ne veulent pas se plonger dans des rapports PDF de plus de cent pages. Ils ne souhaitent pas lire les bienfaits d’un outil non-pertinent. Et il est peu probable que les développeurs assistent à un séminaire en ligne de 90 minutes à 9h du matin pour examiner les résultats d’un test d’intrusion.

Pour toutes ces raisons, il existe des plateformes mettant en relation les développeurs et les hackers informatiques en temps réel. Certaines plateformes de bug bounty permettent de “tagger” les personnes, d’attribuer une vulnérabilité à différents groupes et d’insérer des sous-traitants et fournisseurs à un rapport. Une méthode qui contribue à rendre la communication et la collaboration aussi optimisées et simples que possible.

Tandis que “le logiciel dévore le monde” et que l’interconnexion des systèmes devient la norme, penser qu’il est possible de sécuriser ses systèmes en interne s’apparente à une vision dépassée de la sécurité. Bien évidemment, la découverte et la divulgation de vulnérabilités doit être gérée différemment pour une entité militaire, un service public, une entreprise du secteur industriel ou un simple site vitrine. Mais toutes les organisations, quelle que soit leur taille, peuvent bénéficier des avantages offerts par la sécurité collaborative. Le bug bounty est la partie la plus visible de cette sécurité mais elle n’est pas la seule. Les options sont nombreuses et la qualification des vulnérabilités demande temps et expertise. Pour ces raisons, lorsque l’on souhaite améliorer la sécurité de sa plateforme ou de son applicatif, il est important de bien comprendre les options possibles et de se faire accompagner. □

HackerOne est la plateforme collaborative numéro un de pentest & de bug bounty, qui permet aux organisations de trouver et corriger les vulnérabilités critiques avant qu’elles ne soient exploitées grâce à une communauté internationale d’hackers éthiques.

Pour plus d’informations :
www.hackerone.com

hackerone

HACK FOR GOOD

"Find the bugs before the bad guys do."

@randomdeduction

#TOGETHERWEHITHARDER

WWW.HACKERONE.COM / WWW.HACKER101.COM


Attackers start with people.
Your protection should, too.
Proofpoint protects your people, data and systems by stopping threats, training users and securing information everywhere it lives.
Visit proofpoint.com to find out more.
proofpoint.
Protection starts with people.

Cybermenaces internes : Se défendre contre l'erreur humaine

Quels que soient les outils et les contrôles que nous mettons en place, nous n'éradiquerons jamais l'erreur humaine.

Par Loïc Guézo

Les menaces internes sont particulièrement difficiles à détecter. Empêcher les cybercriminels d'infiltrer son système est une tâche compliquée, mais se défendre contre ceux qui en font déjà partie est une toute autre affaire. Une menace interne n'a pas besoin de contourner les systèmes de défense, elle n'éveille aucun soupçon et passe souvent inaperçue. En moyenne, il faut 77 jours pour repérer et contenir un incident interne.

Toutes les formes de menaces internes sont en augmentation. L'année dernière, elles ont coûté aux entreprises 11,45 millions de dollars, soit une hausse de 31 % par rapport à 2018.

Si les conséquences de ces menaces peuvent être dévastatrices, les auteurs des menaces internes n'ont généralement aucune intention malveillante. Près des deux tiers des incidents internes signalés l'année dernière concernaient la négligence d'employés ou d'entrepreneurs. En d'autres termes, il s'agit simplement d'une erreur humaine.

Chiffrer le coût des collaborateurs négligents

Une menace interne n'a pas besoin d'être accompagnée d'une quelconque intention malveillante pour causer des dommages importants. De nombreuses entreprises mondiales ont fait les frais de la négligence de leurs collaborateurs et de leurs sous-traitants. L'énorme fuite de données d'Equifax en 2017 a été causée en partie par des employés qui selon les termes du PDG de l'entreprise, « *n'ont pas tenu compte des avertissements de sécurité* ». Dans son examen officiel de l'incident, le PDG américain a attribué une grande partie de la responsabilité à des contrôles internes insuffisants et à l'incapacité de mettre en œuvre les meilleures pratiques de sécurité.

Toutes les entreprises sont exposées à des menaces internes, en particulier lorsqu'il s'agit d'actes involontaires. Quels que soient les outils et les contrôles que nous mettons en place, nous n'éradiquerons jamais l'erreur humaine.

Cependant, tous les incidents ne sont pas causés par des défaillances systématiques. Certains peuvent être déclenchés par une simple erreur humaine. Le phishing notamment, reste un problème majeur pour les équipes de cybersécurité. Plus de la moitié des entreprises ont été victimes d'une attaque réussie l'année dernière, mais malgré son omniprésence, seuls 61 % des travailleurs dans le monde connaissent ce terme.

Il suffit qu'un employé clique sur un lien malveillant pour provoquer des dégâts financiers colossaux et nuire gravement à la réputation de l'entreprise - comme peut en témoigner Sony Pictures. L'entreprise a dépensé 35 millions de dollars pour réparer ses systèmes informatiques en 2014, après que plusieurs cadres supérieurs aient été victimes de phishing. Les attaquants ont divulgué des informations sur la propriété intellectuelle et des e-mails sensibles, et ont volé plus de 100 téraoctets de données.

La perte des codes d'accès d'un utilisateur privilégié, que ce soit par le biais du phishing ou par tout autre moyen, peut avoir un impact dévastateur. Une fois compromis, les codes d'accès peuvent être utilisés sur des périodes prolongées pour accéder à des informations sensibles, détourner des fonds, paralyser des réseaux et bien plus encore.

Quelle que soit la nature d'une menace interne, sa durée est proportionnelle à son impact : plus longtemps elle reste non détectée, plus le prix à payer est élevé. Celles contenues dans les 30 jours coûtent en moyenne 7,12 millions de dollars, tandis que celles qui prennent plus de 90 jours pour être contenues coûtent en moyenne 13,71 millions de dollars.

Les collaborateurs mettent-ils votre entreprise en danger ?

Toutes les entreprises sont exposées à des menaces internes, en particulier lorsqu'il s'agit d'actes involontaires. Quels que soient les outils et les contrôles que nous mettons en place, nous n'éradiquerons jamais l'erreur humaine. Elle fait partie de chacun d'entre nous. Cependant, plus l'entreprise est grande, plus le risque est grand - et plus les conséquences sont graves.

Le nombre de menaces internes a augmenté en fonction des effectifs, tout comme l'impact financier. Les entreprises comptant entre 25 000 et 75 000 employés ont dépensé en moyenne 17,92 millions de dollars au

Donnez à votre personnel les compétences et les connaissances nécessaires pour protéger votre entreprise. La formation doit couvrir un large éventail de sujets, il s'agit de bien plus qu'un simple exercice de cotation.

cours de l'année dernière pour traiter des incidents internes, contre 6,92 millions de dollars pour les entreprises comptant entre 500 et 1 000 employés.

Le facteur de risque le plus important en ce qui concerne les collaborateurs négligents est l'absence de connaissance. Les utilisateurs finaux, à tous les niveaux et dans tous les secteurs, sont insuffisamment informés des risques courants et de leur rôle dans la défense contre ceux-ci. La cause ? Un manque de formation continue et complète des collaborateurs.

Selon un rapport, 68 % des cadres et des dirigeants ne comprennent pas bien les menaces persistantes et la manière dont elles peuvent avoir un impact négatif sur les entreprises. Pire encore, 60 % ne comprennent pas que les cyberattaques sont une préoccupation constante.

Défendre directement de l'intérieur

La lutte contre les menaces internes est un processus complexe. En particulier lorsque les "agresseurs" n'ont pas l'intention de commettre une attaque. Si les menaces peuvent être difficiles à définir, elles sont encore plus difficiles à détecter.

Toute défense doit se concentrer sur trois domaines clés : votre technologie, vos processus et, surtout, votre personnel. Toutes les entreprises doivent mettre en place des solutions pour surveiller l'activité des utilisateurs et signaler toute demande inhabituelle et tout accès au système. Utilisez les outils et la technologie pour limiter l'accès aux informations sensibles et pour interdire la copie ou l'exportation de ces données.

Cette technologie doit être soutenue par des processus clairement définis et faciles à suivre concernant tout, de la gestion des appareils à l'accès au réseau et à l'utilisation acceptable. Les employés doivent être conscients des conséquences du non-respect de ces politiques.

Enfin, donnez à votre personnel les compétences et les connaissances nécessaires pour protéger votre entreprise. La formation doit couvrir un large éventail de sujets, il s'agit de bien plus qu'un simple exercice de cotation.

Si vos employés ne font pas de simulations d'attaques ou ne participent pas régulièrement à des ateliers de sécurité, votre formation est probablement insuffisante. S'ils ne comprennent pas la menace que représente la négligence pour votre entreprise ou s'ils ne sont pas conscients du rôle qu'ils jouent dans la défense contre les cyberattaques, alors votre entreprise est certainement en danger. □

Loïc Guézo, Directeur Stratégie Cybersécurité, SEMEA, Proofpoint.

Pour plus d'informations :
www.proofpoint.com/fr

proofpoint.

Bonnes pratiques de la sécurité des connexions à distance

La possibilité de travailler depuis n'importe où améliore la flexibilité et la productivité. Mais tout n'est pas aussi rose pour les professionnels de l'informatique qui doivent mettre en place l'infrastructure nécessaire pour soutenir le télétravail.

Par Netwrix

Avec l'explosion des technologies Cloud et la généralisation de l'Internet à haut débit, de nombreuses organisations permettent à leurs employés de travailler à distance. Après tout, la possibilité de travailler depuis n'importe où améliore la flexibilité et la productivité. Mais tout n'est pas aussi rose pour les professionnels de l'informatique qui doivent mettre en place l'infrastructure nécessaire pour soutenir le télétravail. Alors qu'ils s'efforcent d'assurer un accès ininterrompu aux services et aux applications, d'autres projets importants sont mis en attente, notamment des initiatives essentielles liées à la sécurité. Les cybercriminels savent que les organisations sont plus vulnérables que jamais et multiplient leurs attaques.

Checklist 1 : Rendre votre configuration de télétravail aussi sûre que possible

Quel que soit le stade où vous en êtes dans la mise en place de votre infrastructure de soutien au télétravail, voici quelques précieux conseils pour la rendre aussi sûre que possible :

- Dans la mesure du possible, utilisez des appareils gérés. Pour chaque appareil qui se connecte à votre réseau :
  - Activez le chiffrement en utilisant BitLocker pour Windows et FileVault pour MacOS.
  - Installez un antivirus et un pare-feu.
  - Veillez à ce que tous les systèmes d'exploitation et les logiciels bénéficient du support technique du fournisseur.
  - Tenez à jour tous les systèmes d'exploitation et logiciels, en installant toutes les mises à jour importantes.
  - Appliquez la stratégie de mots de passe, désactivez la connexion automatique et activez le verrouillage automatique.
  - Activez la fonction « Trouver mon appareil » et les fonctions de verrouillage et d'effacement à distance.
- Si vous n'êtes pas en mesure d'utiliser des appareils gérés, fournissez à tous les employés un guide de sécurité qui explique les mesures de sécurité obligatoires et recommandées pour les travailleurs à distance.
- Dispensez régulièrement à vos employés des formations de sensibilisation aux menaces.
- Utilisez le VPN – n'oubliez pas que vos employés sont susceptibles d'utiliser les réseaux WiFi publics.
- Si possible, utilisez l'authentification multifacteur (MFA) pour protéger les comptes VPN et les services Cloud contre les accès non autorisés.
- Évitez d'utiliser le protocole RDP (Remote Desktop Protocol). Si vous devez utiliser le RDP :
  - N'exposez pas le RDP à Internet. Toutes les activités doivent s'effectuer via une connexion sécurisée.
  - Évitez les connexions RDP directes. Il est conseillé de forcer les sessions RDP via la passerelle Remote Desktop Gateway, idéalement dans une zone démilitarisée (DMZ).
  - Restreignez l'accès au RDP à une liste blanche d'utilisateurs et de serveurs.
- N'utilisez pas les numéros de port par défaut lorsque vous établissez des connexions à distance.
- Si possible, limitez l'accès à distance à une liste blanche d'adresses IP connues et fiables.
- Chaque fois que possible, désactivez les accès « tout le monde » et « anonyme ».

Si vous n'êtes pas en mesure d'utiliser des appareils gérés, fournissez à tous les employés un guide de sécurité qui explique les mesures de sécurité obligatoires et recommandées pour les travailleurs à distance.

Checklist 2 : Atténuer les risques liés à l'accroissement de votre surface d'attaque

En suivant les étapes de la checklist précédente, vous contribuerez à rendre votre environnement plus sûr, mais votre surface d'attaque restera plus grande que jamais. Suivez les bonnes pratiques ci-dessous pour réduire encore le risque de violations et d'autres incidents de sécurité :

- Respectez les bonnes pratiques élémentaires en matière de gestion de l'environnement informatique. En particulier :
  - Identifiez tous les comptes périmés et inutilisés, puis supprimez-les ou désactivez-les.

Veillez à ce que votre stratégie de mots de passe soit bien configurée. Vérifiez vos exigences en matière de longueur et de complexité, et privilégiez les mots de passe faciles à retenir et difficiles à deviner.

  - Vérifiez toutes les autorisations et supprimez les droits excessifs et inutilisés, notamment les droits d'accès à distance.
  - Réduisez le nombre de comptes privilégiés.
  - Remaniez votre modèle de délégation AD.
  - Arrêtez ou désinstallez les services réseau inutilisés.
  - Affinez votre stratégie de groupe.
- Veillez à ce que votre stratégie de mots de passe soit bien configurée. Vérifiez vos exigences en matière de longueur et de complexité, et privilégiez les mots de passe faciles à retenir et difficiles à deviner.
- Mettez en place une politique de verrouillage des comptes visant à empêcher les pirates de pénétrer dans votre réseau en devinant le mot de passe d'un utilisateur. Mais ne réduisez pas le nombre de tentatives infructueuses autorisées avant verrouillage à tel point que cela cause de la frustration et une perte de productivité aux utilisateurs légitimes (qui peuvent faire des fautes de frappe occasionnelles).
- Utilisez les groupes d'Active Directory et Azure AD pour contrôler l'accès à votre infrastructure. Contrôlez régulièrement vos groupes et les appartenances aux groupes, pour garantir que personne ne dispose d'autorisations excessives.
- Assurez-vous que les autorisations NTFS et les droits d'accès aux ressources partagées comme SharePoint, SharePoint Online, OneDrive for Business et Teams respectent le principe du moindre privilège.
- Respectez les bonnes pratiques d'audit dans chacun des domaines suivants :
  - *Audit des configurations* – Veillez à ce que la configuration de toutes les ressources critiques soit conforme à votre niveau de sécurité de référence, et vérifiez toutes les modifications apportées aux configurations pour détecter les erreurs et les activités malveillantes.
  - *Audit des accès* – Surveillez les connexions aux ressources dans le Cloud et sur site, ainsi que les connexions au VPN.
  - *Audit des activités* – Surveillez les activités des utilisateurs relatives aux données, en particulier celles qui concernent les données sensibles et les solutions Cloud qui soutiennent le travail à distance, telles que SharePoint Online, OneDrive for Business et MS Teams. Faites preuve de vigilance vis-à-vis de l'appartenance à des groupes suspects et des modifications apportées aux autorisations qui pourraient indiquer une augmentation de privilèges. Soyez à l'affût des pics d'activités suspectes au niveau des ports de votre réseau et des connexions VPN, notamment les scans de ports et les tentatives de connexion échouées, qui peuvent être le signe d'attaques par pulvérisation de mots de passe ou par force brute.
- Évaluez les risques à l'échelle de l'entreprise. Soyez particulièrement attentif à vos services distants.
- Rédigez vos politiques et diffusez-les à tous ceux qui accèdent à votre environnement informatique. □

Pour plus d'informations :
www.netwrix.com

netwrix

Forthcoming events

SECURING
FINANCIAL SERVICES
VR

8th July 2020
Online

e-crime & cybersecurity NORDICS VR

23rd September 2020
Online

e-crime & cybersecurity MID-YEAR VR

15th October 2020
Online

e-crime & cybersecurity MIDDLE EAST VR

21st October 2020
Online

e-crime & cybersecurity SPAIN VR

17th November 2020
Online

e-crime & cybersecurity BENELUX VR

1st December 2020
Online

For more information, please call Robert Walker on +44 (0)20 7404 4597
or email robert.walker@akjassociates.com

2020: L'année du Phishing COVID (... et bien plus encore...)

Dans notre rapport Cofense Q1 2020 Phishing, nous dévoilons l'état actuel du phishing.

Par Andy Spencer

En 2020, les pirates continuent de faire ce qu'ils font de mieux : trouver des moyens de se faufiler au travers des passerelles de messagerie sécurisées (Secure Email Gateway – SEG) pour délivrer des menaces aux utilisateurs. Dans notre rapport Cofense Q1 2020 Phishing, nous dévoilons l'état actuel du phishing : un mélange créatif de nouveaux et anciens mécanismes de livraison, de thèmes et de logiciels malveillants, principalement conçus pour exploiter la pandémie de COVID-19. Faisons un petit point ensemble sur nos conclusions et ce qu'elles laissent présager pour le reste de l'année.

Récapitulatif

L'année a commencé avec une accalmie pré-vacances dans le volume total de logiciels malveillants. À la fin du mois de février, un pic spectaculaire a démarré quand les pirates ont commencé à profiter du COVID-19 comme thème lucratif et convaincant de phishing. Emotet, qui a repris ses activités à la mi-janvier, a chuté un mois plus tard à mesure que le virus se propageait à l'échelle mondiale. Les pirates ont tout-suite intensifié le thème de phishing COVID qui a pris de l'ampleur tout le mois de Mars.

Se faisant passer pour des autorités, les attaquants ont envoyé des messages urgents délivrant des logiciels malveillants. Nombreux messages ont atteint les utilisateurs au moment où ils s'adaptaient à une nouvelle norme de télétravail, simulant des changements interne ou usurpant des services informatiques en offrant « du support » aux utilisateurs.

Cofense a découvert deux familles de ransomware délivré par des campagnes COVID ciblant les hôpitaux. Les opérateurs malicieux ont redoublé leurs efforts au premier trimestre, combinant parfois une infection ransomware avec une violation de données et libération d'informations sensibles si un paiement n'était pas effectué. Nous avons constaté des tactiques subversives qui ont permis aux courriels de Phishing COVID de délivrer ces ransomwares en passant inaperçus au travers des SEGs bien connus.

Alors que les documents Microsoft Office portant des macros malveillantes étaient toujours le meilleur mécanisme de livraison, d'autres ont eu un impact, comme des téléchargeurs malveillants et le nouveau GuLoader utilisé pendant COVID. Au plus les organisations adoptent des solutions Cloud, au plus les pirates augmentent leurs malices pour délivrer des « Payloads ». Les États-Unis continuent d'héberger le plus de serveurs C2, ce qui n'est pas surprenant étant donné l'infrastructure disponible pour l'Amérique.

A quoi s'attendre ?

Dans la nouvelle « normalité », faites attention aux thèmes novateurs de phishing qui continuent de jouer sur l'émotion du moment : invitations à des demandes de collecte sociale, avis de décès, et messages de relance financière.

Cofense anticipe une croissance continue de ransomware. Les cibles habituelles doivent rester vigilantes : secteur de la santé et collectivités locales ; en fait les industries vulnérables avec un budget de sécurité plus modeste.

De nouvelles cibles peuvent émerger. Comme les attaques réussies font la une de l'actualité, on peut s'attendre à une augmentation du ransomware avec exfiltration de données, l'idée étant d'augmenter la pression extorsionniste. Les compagnies d'assurance cybersécurité encourageant souvent les paiements, cette tendance peut se poursuivre.

Pour sûr : les e-mails de phishing échapperont aux SEGs les plus avancés et atteindront les utilisateurs. C'est simplement une question de temps. Les organisations doivent reconnaître, et s'assurer que leur stratégie de défense intègre à la fois l'intuition humaine ainsi que la technologie automatisée pour mener une lutte contre le Phishing efficace. Les utilisateurs sont, plus que jamais, en première ligne de la cyberdéfense. □

Andy Spencer, VP, Sales Engineering, Cofense.

Cofense®, le leader mondial des fournisseurs de solutions de défense contre le phishing, unit l'humanité contre le phishing. La gamme de produits Cofense englobe des informations en temps réel sur les attaques qui ont échappé aux périmètres de sécurité traditionnels et qui ont été signalé par les employés, avec les meilleures technologies de sécurité opérationnelles dans leur catégorie pour arrêter les attaques rapidement et garder une longueur d'avance sur les violations.

Pour en savoir plus, cofense.com ou rejoignez-nous sur Twitter et LinkedIn.


VOTRE « EMAIL GATEWAY »
EST-IL VRAIMENT SÉCURISÉ?
Tous les jours, Cofense détecte des menaces de phishing dans les environnements protégés par des Email Gateway «sécurisés».
Quel est VOTRE plan pour les arrêter?
COFENSE
Découvrez comment nous pouvons vous aider à attraper les emails de phishing dans votre boîte de réception et évitez une brèche.
cofense.com

www.cyberviser.com

You know AKJ Associates for its 20-year record of market-leading conferences and events in cybersecurity and compliance. Under the e-Crime Congress, Securing the Law Firm and PCI London brands, we have consistently tried to get ahead of the trends shaping your market and careers, instead of rehashing the same old ideas.

We were first to bring CFOs and institutional investors to you, to reveal what business and stakeholders really think about cyber. We were at the forefront of understanding the collision of cybersecurity, operational risk and compliance. And we have not been afraid to confront cybersecurity's many inconvenient truths.

To expand the resources we provide to you, we have launched a website to continue our mission of delivering independent thought leadership, news and views.

www.cyberviser.com brings you:

- ✓ **Research and data:** AKJ Associates' proprietary data and conclusions gathered from security professionals around the globe. Our first project, 'Who Secures the UAE' is now live.
- ✓ **News and comment:** the most significant news stories with interpretation and comment from AKJ editors and the market.
- ✓ **Best practice:** what works and what doesn't, direct from leading end-users and security practitioners.
- ✓ **Regulation:** the latest global news on regulation and compliance, cross-sector, cross-region.
- ✓ **People:** who is firing, who is hiring and what are they paying? CISO profiles and interviews.
- ✓ **Vendors:** start-ups, funding, M&A, new solutions and new technologies.

Sponsors et exposants

CrowdStrike | Sponsor stratégique

CrowdStrike® Inc. (Nasdaq : CRWD), l'un des leaders mondiaux dans le domaine de la cybersécurité, redéfinit la sécurité à l'ère du cloud en proposant une plateforme de protection des postes clients (endpoints) conçue de A à Z pour bloquer les intrusions. Basée sur un agent léger unique, l'architecture de la plateforme CrowdStrike Falcon® utilise la puissance de l'intelligence artificielle (IA) en cloud pour offrir une protection et une visibilité en temps réel d'un bout à l'autre de l'entreprise, prévenant les attaques lancées contre les endpoints, qu'ils soient ou non connectés au réseau. Optimisée par CrowdStrike Threat Graph®, la plateforme CrowdStrike Falcon met instantanément en corrélation plus de deux mille milliards d'événements de sécurité liés aux endpoints par semaine et dans le monde entier, alimentant en données de sécurité l'une des plateformes de protection des données les plus performantes au monde.

Avec CrowdStrike, les entreprises bénéficient d'une protection accrue, de meilleures performances et d'un retour sur investissement immédiat grâce à Falcon, sa plateforme native en cloud. En résumé, CrowdStrike stoppe les menaces et empêche les failles de cybersécurité. Les entreprises peuvent tester Falcon Prevent™ en demandant un essai gratuit.

Pour en savoir plus : www.crowdstrike.com – www.crowdstrike.fr

Darktrace | Sponsor stratégique

Darktrace est leader mondial de l'IA pour la cyberdéfense et le créateur de la technologie de Réponse Autonome.

Son IA auto-apprenante reproduit le système immunitaire humain et est utilisée par plus de 3000 organisations afin de se protéger contre les menaces qui pèsent sur les emails, le cloud, l'IoT, ou encore les réseaux bureautiques et industriels. Cela inclut la menace interne, l'espionnage industriel, la compromission d'IoT, les vulnérabilités zero-day, la fuite de données, les risques liés à la chaîne logistique ou encore les vulnérabilités d'infrastructure sur le long-terme.

Darktrace compte plus de 900 employés et 40 bureaux dans le monde, et son double siège social est présent à San Francisco et Cambridge, Royaume-Uni. Toutes les 3 secondes, l'IA de Darktrace riposte contre une cybermenace, l'empêchant de provoquer des dégâts.

Pour en savoir plus : www.darktrace.com

HackerOne | Sponsor stratégique

HackerOne est la plateforme collaborative numéro un de pentest & de bug bounty, qui permet aux organisations de trouver et corriger les vulnérabilités critiques avant qu'elles ne soient exploitées grâce à une communauté internationale d'hackers éthiques. Avec plus de 1 800 programmes clients, dont le ministère de la défense Américain, General Motors, Google, PayPal, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapour, Starbucks, Dropbox et Intel, HackerOne a aidé à trouver plus de 150 000 vulnérabilités et à distribuer plus de 85 millions de dollars de primes à une communauté croissante de plus de 600 000 hackers. HackerOne a des bureaux à San Francisco, Paris, Munich, Londres, New York, Groningen et Singapour.

Pour en savoir plus : www.hackerone.com

Netwrix | Sponsor stratégique

Netwrix est un éditeur de logiciels qui permet aux professionnels de la sécurité et de la gouvernance de l'information de reprendre le contrôle des données sensibles, réglementées et stratégiques, quel que soit leur emplacement.

Plus de 10 000 organisations du monde entier s'appuient sur les solutions Netwrix pour sécuriser leurs données sensibles, tirer pleinement parti des contenus d'entreprise, réussir les audits de conformité et améliorer la productivité de leurs équipes informatiques.

Pour plus d'information sur Netwrix, visitez www.netwrix.fr

Proofpoint | Sponsor stratégique

Proofpoint est une entreprise leader dans le domaine de la cybersécurité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, nous aidons les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web.

Pour plus d'informations, rendez-vous sur www.proofpoint.com/fr

Pulse Secure | Sponsor stratégique

Pulse Secure offre des solutions Secure Access simples, complètes basées sur des logiciels pour les personnes, appareils, objets et services qui améliorent la visibilité, la protection et la productivité de nos clients. Nos solutions et suites logicielles intègrent de manière unique un accès au cloud, aux appareils mobiles, aux applications et au réseau qui assure un système informatique hybride dans un environnement Zéro confiance. Plus de 20 000 entreprises et prestataires de service de tous les secteurs font confiance à Pulse Secure pour donner les moyens à leur employés mobiles d'accéder aux applications et aux informations conservées dans le centre de données et le cloud en toute sécurité tout en garantissant le respect des normes internes aux entreprises.

Par example la solution Pulse Access Suite Plus. Une solution de connectivité protégée, une intelligence opérationnelle et une réponse face aux menaces dans les environnements mobiles, réseaux et multi-clouds afin de fournir une gestion unique transparente aux administrateurs ainsi qu'une simplicité d'utilisation hors du commun aux utilisateurs finaux. L'orchestration et la simplicité de Secure Access sont obtenus par un système de gestion centralisé, une plateforme d'application unifiée, une grande couverture du point d'extrémité client et une infrastructure basée sur les normes et d'interopérabilité dans le cloud.La Suite est conçue pour faciliter les achats grâce à des possibilités d'extension, à un déploiement et un octroi de licence flexibles afin de réduire les coûts totaux de propriété. Elle offre un point d'extrémité dynamique et une surveillance des accès, une application granulaire de la politique en matière d'accès et fonctionne à l'aide d'une infrastructure client existante et un écosystème d'accès. Ainsi, les entreprises peuvent renforcer les outils d'accès au cloud à distance, réduire les risques en matière de sécurité et contrôler les lacunes ainsi gagner en efficacité opérationnelle et faire des économies.

Pour plus d'information, visitez www.pulsesecure.net

SentinelOne | Sponsor stratégique

SentinelOne is the only cybersecurity solution encompassing AI-powered prevention, detection, response and hunting across endpoints, containers, cloud workloads, and IoT devices in a single autonomous platform. With SentinelOne, organisations gain full transparency into everything happening across the network at machine speed – to defeat every attack, at every stage of the threat lifecycle.

To learn more, visit www.sentinelone.com

Bitglass | Sponsor du séminaire de formation

Bitglass, la société CASB de nouvelle génération, basée dans la Silicon Valley et possède des filiales sur tous les continents. La solution de sécurité Cloud de Bitglass offre une protection immédiate des données contre les menaces, pour toutes les applications, pour tout type de périphériques, pour tout type de connexions et cela sans agent.

Avec la prise en charge des applications sanctionnées telles qu' Office 365, GSuite et AWS, ainsi que des applications non gérées telles qu'un Dropbox et/ou des réseaux sociaux, Bitglass est conçu pour protéger les données en temps réel dans vos applications d'entreprise les plus critiques. Les applications non gérées sont automatiquement détectées et peuvent facilement être sanctionnées à partir de la console d'administration. Seul Bitglass assure la protection des données en temps réel, la protection contre les menaces, la gestion des identités et la visibilité, le tout sans agent.

Pour plus d'information, visitez www.bitglass.com

BitSight | Sponsor du séminaire de formation

BitSight transforme la façon dont les organisations gèrent le cyber-risque. La plate-form de notation de sécurité BitSight applique des algorithmes sophistiqués, produisant des cotes de sécurité quotidiennes allant de 250 à 900, pour aider les organisations à gérer leurs propres performances de sécurité; atténuer le risque de tiers; souscrire des polices d'assurance cyber; mener une diligence financière; et évaluer le risque global. Avec plus de 2 100 clients dans le monde et le plus grand écosystème d'utilisateurs et d'informations, BitSight est la norme en matière de notes de sécurité.

Pour plus d'informations, veuillez visiter www.bitsight.com, lire notre blog ou suivre @BitSight sur Twitter

Cofense | Sponsor du séminaire de formation

Cofense®, le leader mondial des fournisseurs de solutions de défense contre le phishing, unit l'humanité contre le phishing. La gamme de produits Cofense englobe des informations en temps réel sur les attaques qui ont échappé aux périmètres de sécurité traditionnels et qui ont été signalé par les employés, avec les meilleures technologies de sécurité opérationnelles dans leur catégorie pour arrêter les attaques rapidement et garder une longueur d'avance sur les violations. Les clients de Cofense incluent les organisations « Global 1000 » dans les secteurs de la défense, de l'énergie, des services financiers, de la santé et de la fabrication. Ces clients comprennent que conditionner les utilisateurs au bon comportement, améliorera la sécurité, facilitera la réponse aux incidents et réduira le risque.

Pour en savoir plus, cofense.com ou rejoignez-nous sur Twitter et LinkedIn

Cybereason | Sponsor du séminaire de formation

Cybereason is the leader in endpoint protection, offering endpoint detection and response, next-generation antivirus, and managed monitoring services. Founded by elite intelligence professionals born and bred in offence-first hunting, Cybereason gives enterprises the upper hand over cyber adversaries. The Cybereason platform is powered by a custom-built in-memory graph, the only truly automated hunting engine anywhere. It detects behavioural patterns across every endpoint and surfaces malicious operations in an exceptionally user-friendly interface. Cybereason is privately held and headquartered in Boston with offices in London, Tel Aviv, and Tokyo.

For more information, please visit www.cybereason.com

Cybersel | Sponsor du séminaire de formation

Cybersel a été fondée en 2011, le spin-off d'une société qui existait depuis le 2003 spécialisée dans l'exploitation informatique.

Animée par la même équipe d'experts, Cybersel possède une longue expérience pour accompagner les directions informatiques des grandes entreprises.

Notre mission, est d'identifier au niveau international les technologies les plus avancées et les plus innovantes afin de les proposer à nos clients sur notre marché historique en Italie, et plus récemment en France et en Angleterre où nous avons ouvert des filiales en 2019.

Notre modèle commercial s'apparente à celui d'un « comptoir » des technologies de pointe dans le segment de la cyber sécurité :

- Une offre des meilleures solutions commercialisées à travers des partenariats forts qui sont garants de la représentation locale des éditeurs.
- Un service de consultants opérationnels et de proximité pour former, accompagner nos clients dans la mise en œuvre de ces solutions, et les utiliser de manière optimale.

La croissance et l'évolution exponentielle des cyberattaques au cours des dernières années a considérablement développé l'intérêt des entreprises sur ces sujets, les amenant à concevoir et mettre en œuvre des stratégies de plus en plus complexes et sophistiquées.

C'est pourquoi Cybersel est spécialisée dans l'apport de solutions pour aider les entreprises à faire face aux défis de plus en plus aigus que représentent les cybers attaques.

La gestion des risques cybernétiques, l'analyse des postures en matière de cyber-sécurité et la simulation d'attaques sur lesquels nous accompagnons quotidiennement nos clients.

Pour plus d'information, visitez cybersel.co.uk

Digital Shadows | Sponsor du séminaire de formation

Digital Shadows réduit les risques numériques en identifiant les expositions indésirables et en protégeant contre les menaces externes. Lorsque les risques numériques ne sont pas adressés, une entreprise peut faire face à des amendes pour non-conformité, une atteinte à sa réputation, ou encore à des pertes de propriété intellectuelle. La plateforme SearchLight de Digital Shadows vous aide à réduire ces risques en détectant vos pertes de données, en sécurisant votre présence en ligne et en réduisant votre surface d'attaque.

Pour plus d'information, visitez www.digitalshadows.com

Synack | Sponsor du séminaire de formation

Synack offers a new and revolutionary security testing platform, designed to locate and fix critical vulnerabilities in business-critical applications and infrastructures that would otherwise go undetected. Synack provides customers with large teams of international, top-class security experts who check the IT assets on the customer side – taking a multi-layered and contraindicative approach – and often reveal vulnerabilities within hours. That, combined with the development of a self-learning, data analysis-based reconnaissance technology and a transparent, AI-based platform with a real-time customer portal, makes Synack a provider of an innovative and effective method for security tests. This next generation test platform overcomes the deficits of conventional penetration tests and security risk testing. In addition, it offers the advantage of unprecedented simulations of increasingly complex cyber-attacks and TTPs, i.e. tactics, technology and procedures. Synack keeps its customer base confidential. These include some of the largest F500 / G500 groups, including banks and financial service providers, retailers, healthcare professionals, consumer goods companies, manufacturing and technology companies, and the U.S. government (the Department of Defense / Hack the Pentagon project, the IRS tax authority). Synack was founded in 2013 by former NSA security expert Jay Kaplan, CEO of the company, and Dr. Mark Kuhr, in the role of CTO. Synack offers its solution in the form of a subscription to ongoing security tests – to ensure the protection of business-critical assets. For assets that require timely tests, there is the option of a 14-day security test.

To learn more, visit our website at http://www.synack.com

Terranova Security | Sponsor du séminaire de formation

Terranova Security est un chef de file mondial et un partenaire de choix pour la formation en sensibilisation à la sécurité. Ses programmes de sensibilisation à la sécurité et de simulation de phishing ont formé plus de 10 millions d'utilisateurs. L'entreprise est reconnue pour son contenu de qualité supérieure, son portfolio de formations et d'outils de communication multilingues, sa plateforme intuitive de sensibilisation à la sécurité et de simulation de phishing. Les organisations continuent de tirer profit de la démarche en cinq étapes en sensibilisation à la sécurité de Terranova Security, qui propose une approche étape par étape, basée sur les faits, pour mettre en œuvre un programme de sensibilisation à la sécurité réussi. Terranova Security travaille avec des organisations et des équipes de sensibilisation à la sécurité à travers le monde pour concevoir des programmes qui contribuent à réduire considérablement le facteur de risque humain et prévenir efficacement toute cyberattaque.

Pour en apprendre davantage, visitez le terranovasecurity.com

Tripwire | Sponsor du séminaire de formation

Les solutions Tripwire pour la sécurité et la conformité IT aident les organisations à garder le contrôle sur leur infrastructure informatique. Qu'il s'agisse de garantir la conformité et l'application des normes, de détecter les menaces ou de transformer les données relatives à la sécurité en informations exploitables pour les dirigeants de l'entreprise, Tripwire a la solution qu'il vous faut.

Pour plus d'information, visitez www.tripwire.com

AGENDA

08:00 Connexion et session de networking

08:55 Les mots de bienvenue du Président de Conférence

09:00 **Dans un monde digitalisé, on ne peut pas parler de fraude sans parler de cybercriminalité**

Yves Destrebecq, Responsable prévention contre la fraude, HSBC France

- Panorama des principales menaces
- La relation entre la lutte contre la fraude et la cybersécurité
- La mise en place d'un dispositif efficace
- Quand la technologie permet de bloquer les principales menaces : monitoring de la fraude, machine learning, biométrie...

09:20 **Le défi de la chasse aux menaces : Détection, Prévention, Réponse et Chasse – Chaque seconde, chaque jour**

Jan Tietze, Director Security Strategy EMEA, SentinelOne

- Apprenez comment les technologies de détection et de réponse des endpoints (EDR) se mettent en place là où les technologies antivirus s'arrêtent
- Comprenez pourquoi l'EDR devrait être un élément essentiel de chaque stratégie de sécurité des endpoints
- Découvrez comment l'EDR immunise automatiquement les endpoints contre les menaces nouvellement découvertes et fournit un rapport forensic riche, atténue les menaces et isole le réseau des risques

09:40 **IA offensive vs IA défensive : La bataille des algorithmes**

Guilhem Labourel, Account Executive, Darktrace

Parmi les progrès technologiques en évolution rapide, l'émergence de logiciels malveillants améliorés par l'IA rend les cyberattaques exponentiellement plus dangereuses et plus difficiles à identifier. Nous commençons à voir des cyberattaques alimentées par l'IA et exploitées à grande échelle. Pour se protéger contre les attaques de l'IA offensive, les organisations se tournent vers la cyber AI défensive, qui peut identifier et neutraliser les activités malveillantes émergentes, peu importe où et quand elles se produisent.

Dans cette session, découvrez :

- Les changements de paradigme dans le cyber-paysage
- Les progrès dans les techniques d'attaque offensive de l'IA
- L'approche du système immunitaire en matière de cybersécurité et les capacités de réponse autonome et défensive
- Des exemples concrets de menaces émergentes qui ont été arrêtées grâce à la Cyber IA de Darktrace

10:00 **La cyberguerre économique**

Federico Smith, Expert Consultant Cybercrime & Cybersecurity, Council of Europe

- Cyberguerre, cybercriminalité : les dommages collatéraux pour les entreprises
- L'évolution du droit national et international face à la digitalisation du crime organisé
- Les nouveaux moyens de financiarisation du crime organisé 3.0

10:20 **Education Seminars | Session 1**

Cybereason

Comment se défendre contre les attaquants les plus sophistiqués : UNE CYBER-ATTAQUE EN DIRECT EN PLUSIEURS ÉTAPES

Vincent Meysonnet, Senior Sales Engineer, Cybereason

Terranova Security

Priorisez vos utilisateurs: Comment la sensibilisation à la cybersécurité peut aider votre personnel à mieux se protéger contre les cybermenaces lorsqu'ils travaillent à distance

Theo Zafirakos, CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

10:50 Session de networking

11:20 **Les normes faces au cyber-risque**

Paul Steiner, Responsable Conformité SI, La Française des Jeux

- Les normes et le benchmarking de cyber-risque
- La relation entre la cybersecurité et la conformité
- La gestion du cyber-risque. Comment protéger les données de vos utilisateurs ?

11:40 **Augmenter la capacité du télétravail au-delà de la pandémie : comment gérer les problèmes de sécurité**

Xavier Mell, Country Manager – France et Pays d'Afrique parlant français, Pulse Secure

- Malgré les problèmes de sécurité résultant de l'augmentation récente des initiatives de télétravail, un tiers des entreprises ont observé des gains de productivité et 84% d'entre elles prévoient une adoption plus large et plus permanente du télétravail au-delà de la pandémie
- Cette présentation offrira une perspective approfondie des défis, des préoccupations, des stratégies et des résultats escomptés du télétravail
- Découvrez les résultats du rapport 2020 sur la cybersécurité et télétravail et découvrez comment Pulse Secure aide les entreprises à améliorer l'accès sécurisé pour les télétravailleurs

11:50 **Combattez les pirates depuis votre canapé : 5 règles à connaitre !**

Joel Mollo, Regional Director, South EMEA, CrowdStrike

- Le Covid-19 a transformé nos vies, tant personnelles que professionnelles
- Les Cyber-attaquants se sont adaptés, et confrontent ainsi les dirigeants d'entreprise à de nouveaux problèmes
- Venez découvrir comment les contrer dans ce nouveau monde en perpétuelle mutation

12:10 — **Education Seminars | Session 2**

BitSight
Comment BitSight prend en compte les nouveaux cyber risques induits par la généralisation du télétravail ?
Mick Benatek, Business Development Manager – France, Cybersel &
Christophe Leautey, Regional Sales Director, BitSight

Cofense
Préparez vos utilisateurs pour lutter contre l'hameçonnage – Vos équipes sont-elles prêtes à combattre ?
Andy Spencer, VP Sales Engineering, Cofense &
Ekbal Gharbi, Sales Engineer, Cofense

12:40 — **Education Seminars | Session 3**

Digital Shadows
Digital Risk Protection et Télétravail : Détectez la menace avant l'action malveillante !
Tom Sams, Solutions Engineer, Digital Shadows

Tripwire
COVID-19, télétravail et e-commerce : comment les entreprises s'adaptent-elles aux enjeux évolutifs de la cybersécurité ?
Yvan Lanzada, Sales Engineer, Hermitage Solutions SARL on Behalf of Tripwire

13:10 — Déjeuner et session de networking

14:10 — **Traitement des données sensibles : perspectives sur la confidentialité et la sécurité des données au coeur du centre des demandes de visa**

Entretien avec : **Frederik Rouleau,** Architecte de Solutions, TLScontact

14:30 — **Cinq choses à savoir pour pérenniser la sécurité de vos données dès aujourd'hui**

Thomas Limpens, Solution Engineer South-West-Europe, Netwrix

- Êtes-vous prêt à faire face aux menaces qui vont peser sur votre organisation au cours de l'année à venir ?
- Comment allez-vous protéger vos données sensibles et stratégiques contre les utilisateurs malveillants, les rançongiciels et autres attaques, sans oublier les oublis d'administrateurs informatiques débordés ?
- Découvrez 5 astuces qui vous aideront à orchestrer votre sécurité informatique en vous centrant sur les données, ce qui vous donnera une longueur d'avance sur toutes ces menaces et vous permettra d'établir une feuille de route intelligente pour protéger votre entreprise.

14:50 — **Demystifier le Bug Bounty #6 principaux mythes**

Hugues Masselin, Bug Bounty Specialist, HackerOne

It will cover the following 'myths':

- Les programmes de Bug Bounty sont nécessairement publics
- Les programmes de Bug Bounty sont nécessairement annuels & continus
- Le seul moyen de travailler avec les hackers est de les rémunérer
- Le Bug Bounty n'encourage pas la coopération entre développeurs et hackers
- Le Bug Bounty va faire exploser mon budget
- Le Bug Bounty va encourager les hackers à me pirater

15:10 — **Une approche centrée sur l'humain pour gérer les menaces internes**

Gaëtan Gesret, Southern Europe Solutions Engineer, Proofpoint

- Toute personne disposant d'un accès légitime et fiable aux systèmes et aux données d'une organisation peut devenir une menace interne. De ce fait, comment les entreprises peuvent-elles y faire face ?
- Comment une visibilité totale peut-elle fournir le contexte nécessaire pour comprendre et limiter les menaces internes sans sacrifier la confidentialité et la conformité des utilisateurs ?
- Les différents types de menaces internes et les étapes à suivre pour créer votre propre programme de gestion des menaces
- L'accélération de la réponse aux incidents : comment détecter et analyser immédiatement une activité inhabituelle ?

15:30 — **Education Seminars | Session 4**

Bitglass
Comment sécuriser les télé-travailleurs et les données de votre entreprise
Valentin Jangwa, Regional Sales Director, Southern Region, Bitglass
& **Nicolas Liard,** Solutions Engineer, Bitglass

Synack
Témoignage client : ODDO BHF : Retour d'expérience du test d'intrusion collaboratif avec Synack
Gaël Barrez, Sales Director, Synack &
Willem Peerbolt, CISO, ODDO BHF Group

16:00 — Session de networking

16:20 — **TABLE RONDE D'EXPERT(E)S** — **Les participant(e)s pourront choisir entre les tables rondes suivantes :**

« Les 7 leçons tirées du confinement »
La crise du COVID-19 a joué un rôle déterminant dans le fonctionnement des entreprises. Il fallait éliminer les procédures opérationnelles standards et les remplacer par des méthodes de travail presque entièrement nouvelles. Cependant, la plupart des entreprises n'avaient pas anticipé une situation comme celle-ci dans leur planification de reprise après un sinistre / continuité des activités. Alors que nous sortons de la crise initiale, quelles leçons avons-nous tirées pour maintenir une situation de BAU (Business As Usual) – en toute sécurité – face à l'inattendu ?
Réflexions et perspectives de :
Arnaud Martin, RSSI, Caisse des Dépôts
Vincent Ferran-Lacome, Architecte de la Sécurité de l'Information, L'Oréal
Oren Nadjar, CTO, Groupe français indépendant de cosmétique de luxe

« La protection des données dans la nouvelle normalité »
Pour la majorité des entreprises, la transformation numérique a été un processus graduel au cours de la dernière décennie – jusqu'à présent. Les sociétés étant contraintes de se tourner vers des méthodes de travail axées sur le numérique et d'interagir avec les clients, quelles sont les implications pour la gouvernance et la protection des données ? Comment pouvons-nous faire en sorte que l'entreprise prospère dans ce nouveau monde numérique, sans sacrifier la confidentialité ou la sécurité ?
Une discussion avec :
Amina Bouras, Directrice de la Protection des données, Groupe PRO BTP
Hervé Fortin, Responsable de la Protection des données & RSSI Adjoint, Laboratoires Servier

17:00 — Remarques finales

17:10 — Session de networking

17:30 — Clôture de la conférence

Ateliers pour 2020

A la suite des présentations plénières, une série d'ateliers éducatifs vous sera proposée. Les participants peuvent assister aux ateliers de leur choix.

Session 1 : 10:20–10:50

Cybereason

SESSION 1
10:20–10:50

Comment se défendre contre les attaquants les plus sophistiqués : UNE CYBER-ATTAQUE EN DIRECT EN PLUSIEURS ÉTAPES

Vincent Meysonnet, Senior Sales Engineer, Cybereason

Entrez dans le cerveau des attaquants les plus sophistiqués et constatez comment les défenseurs de classe mondiale utilisent leurs compétences et leurs outils de la plus intelligente et efficace des façons. Cette session sera animée par des ingénieurs sécurité de classe mondiale de chez Cybereason, qui sont responsables de la protection des plus grandes organisations du monde. Ils ont récemment annoncé avoir trouvé les solutions contre certaines des récentes attaques sophistiquées de cybersécurité.

Au cours de cette session, nous verrons :

- L'infiltration de l'attaquant ainsi que l'opération malveillante alors qu'elle se déplace dans tout l'environnement de travail
- Le nombre d'opportunités dont dispose un attaquant pour faire avancer l'opération
- Combien d'opportunités le défenseur a-t-il de détruire l'attaque avant d'atteindre sa cible

Terranova Security

SESSION 1
10:20–10:50

Priorisez vos utilisateurs : Comment la sensibilisation à la cybersécurité peut aider votre personnel à mieux se protéger contre les cybermenaces lorsqu'ils travaillent à distance

Theo Zafirakos, CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

Les risques de cybersécurité augmentent lorsque les entreprises adoptent le travail à domicile avec peu de temps pour préparer et informer leurs utilisateurs des risques associés. Alors que certains employés ont peut-être travaillé à domicile dans le passé, pour de nombreux utilisateurs, il s'agit d'un nouvel environnement de travail, en particulier dans les circonstances actuelles. Les cybercriminels savent que de nombreuses personnes s'adaptent à ce nouvel environnement de travail, en confinement, ce qui permet de berner facilement les utilisateurs avec des courriels, des appels et des messages texte. Les fraudeurs profitent de cette situation alors que les utilisateurs tentent de s'adapter au nouvel environnement de travail.

Dans cette session, vous apprendrez pourquoi il est si important de maintenir les programmes de sensibilisation à la cybersécurité et comment atténuer ces cyber menaces liées au télétravail et plus précisément :

- Quels sont les risques de cybersécurité associés au facteur humain lorsque les employés travaillent à distance ?
- Comment les utilisateurs peuvent-ils se défendre et défendre l'entreprise contre l'intensification des cyberattaques ?
- En adoptant une approche centrée sur les personnes: comment la sensibilisation à la cybersécurité peut créer une première ligne de défense ?

Session 2 : 12:10–12:40

Cofense

SESSION 2
12:10–12:40

Préparez vos utilisateurs pour lutter contre l'hameçonnage – Vos équipes sont-elles prêtes à combattre ?

Andy Spencer, VP Sales Engineering, Cofense & **Ekbal Gharbi,** Sales Engineer, Cofense

Alors que le monde est verrouillé pour atténuer les risques de COVID-19, de nombreux employés continuent de s'adapter au travail à domicile, et des entreprises comme la vôtre travaillent dur pour le soutenir. Cependant, les organisations ne peuvent pas verrouiller complètement leurs réseaux. Par exemple, les e-mails de phishing continuent d'échapper aux

passerelles de messagerie sécurisées et les acteurs de la menace adaptant leurs tactiques pour exploiter la crise en cours. Les entreprises sont menacées par une vague de phishing liée au COVID-19 et au travail à distance. Écoutez les experts en sécurité de Cofense Andy Spencer et Ekbal Gharbi qui vont fournir un examen approfondi du paysage actuel des menaces de phishing, tel que vu à travers vos utilisateurs finaux qui sont en première ligne de defense contre le phishing.

Les points saillants comprendront :

- Aperçu de diverses campagnes de phishing qui ont échappé aux SEG et atteint les utilisateurs finaux en fournissant des logiciels malveillants et des attentat de voles les informations d'identification
- Comment les acteurs de la menace utilisent des services de confiance, tels que des enquêtes commerciales en ligne et des plateformes de partage de documents, pour échapper aux SEG
- Prédictions d'experts de ce que nous continuerons de voir jusqu'à la fin du deuxième trimestre et le reste de 2020

BitSight

SESSION 2
12:10–12:40

Comment BitSight prend en compte les nouveaux cyber risques induits par la généralisation du télétravail ?

Mick Benatek, Business Development Manager – France, Cybersel & **Christophe Leautey,** Regional Sales Director, BitSight

Afin de comprendre les risques nouveaux relatifs au déploiement du télétravail, BitSight permet :

- D'apporter une visibilité sur les infections et les vulnérabilités se déroulant sur les réseaux domestiques
- D'analyser la nouvelle surface d'attaque au travers des assets, des providers, des services exposés, y compris les IP des collaborateurs en télétravail
- Identifier et monitorer les tierces parties les plus critiques, avec la mise en place d'une surveillance continue et d'alertes paramétrables en fonction de critères de criticité

Session 3 : 12:40–13:10

Digital Shadows

SESSION 3
12:40–13:10

Digital Risk Protection et Télétravail : Détectez la menace avant l'action malveillante !

Tom Sams, Solutions Engineer, Digital Shadows

Aujourd'hui, obtenir une vue complète et détaillée des menaces qui sont spécifiques à votre entreprise peut représenter un défi considérable. Le télétravail était déjà devenu populaire ces dernières années, mais l'épidémie a forcée de nombreuses organisations à accélérer leurs programmes de transformation du SI et à créer des procédures sur le tas.

Digital Shadows vous présentera :

- Des exemples et des scenarios concrets d'expositions indésirables liées aux risques dont font face la majorité des organisations aujourd'hui
- Pourquoi et dans quelles mesures la prévention des pertes de données et l'acquisition d'intelligence enrichie est critique pour chaque entreprise
- A quel point la détection de telles menaces sur l'Open, Deep et Dark Web permet de réduire et de remédier à ces risques

Tripwire

SESSION 3
12:40–13:10

COVID-19, télétravail et e-commerce : comment les entreprises s'adaptent-elles aux enjeux évolutifs de la cybersécurité ?

Yvan Lanzada, Sales Engineer, Hermitage Solutions SARL on Behalf of Tripwire

Les équipes de sécurité sont à la pointe de la protection de l'entreprise distribuée. La cybersécurité doit être intégrée dans les réponses commerciales basées sur COVID telles que le passage du travail à domicile, la migration vers le commerce électronique et la mise à l'échelle massive de la logistique de livraison. Pour en savoir plus sur la façon dont les professionnels de la sécurité gèrent l'environnement en évolution rapide,

Tripwire a effectué des recherches détaillées et nous aimerions partager certains des résultats fascinants de cette session.

Comprenant :

- Tendances émergentes à travers les régions, la taille de l'entreprise et les niveaux d'emploi sur l'impact de COVID-19 sur les entreprises
- Quels sont les principaux problèmes de sécurité des entreprises ?
- Quelles mesures sont prises pour réduire l'impact de COVID-19 sur les défenses de cybersécurité de leur organisation.
- Quelles technologies sont disponibles pour aider à maintenir la sécurité dans le nouvel environnement de travail

Session 4 : 15:30–16:00

Bitglass

SESSION 4
15:30–16:00

Comment sécuriser les télé-travailleurs et les données de votre entreprise

Valentin Jangwa, Regional Sales Director, Southern Region, Bitglass & **Nicolas Liard,** Solutions Engineer, Bitglass

The world has just observed a surge in remote workers in an era where remote work was already fast approaching. In the long term, we will observe a complex environment that sees an expansion of devices, geographic points of access and access to data outside of traditional boundaries.

Join this webinar to learn how to:

- Enable the short-term surge in remote workers while preparing for a future 'normal'
- How to secure your data, applications, and web interactions from advanced threats
- Secure BYOD devices while enabling productivity
- Identify new access patterns and differentiate between malicious and benign behaviours

Synack

SESSION 4
15:30–16:00

Témoignage client : ODDO BHF : Retour d'expérience du test d'intrusion collaboratif avec Synack

Gaël Barrez, Sales Director, Synack & **Willem Peerbolt,** CISO, ODDO-BHF Group

Cette session présentera le retour d'expérience de Willem Peerbolte, RSSI groupe à ODDO-BHF. Il expliquera pourquoi il a choisi de mettre en place un partenariat avec Synack plutôt que de continuer avec les tests d'intrusions traditionnels. Il présentera ensuite les résultats pour la banque, ses clients et pour lui.

Vous apprendrez :

- Pourquoi ODDO, BHF est passé du test d'intrusion classique aux tests collaboratifs ;
- Comment la plateforme de test de sécurité à distance de Synack contribue à améliorer les pratiques des équipes internes d'ODDO-BHF ; et
- Quels sont les résultats et les avantages que la société obtient □

Intervenants

e-Crime & Cybersecurity France est ravi d'accueillir les participants et les intervenants. L'événement rassemble un grand nombre de personnalités et de décideurs de l'industrie.

Gaël Barrez

Sales Director, Synack

Gaël Barrez est le directeur commercial de Synack. À ce titre, il est chargé de superviser les opérations de Synack en Europe du Sud et en Turquie. Gaël a plus de 20 ans d'expérience dans la vente, le leadership et le développement commercial de la cybersécurité. Il a aidé principalement les 2000 plus grandes entreprises de la région EMEA à protéger leur cœur de métier contre un large éventail de cyber-risques et de menaces terroristes. Il apporte son expertise en matière de sécurité des applications, de sécurité des réseaux, de gouvernance et de gestion des risques, de sécurité du développement logiciel, de cryptographie, de solutions anti-fraude, de PCI-DSS, d'OWASP.

Gaël est titulaire d'un Master en marketing et gestion des technologies de l'information de l'EPITA, une école d'ingénieurs Française. Pendant son temps libre, Gaël aime faire de la plongée sous marine, voyager et apprendre de nouvelles choses.

Mick Benatek

Business Development Manager – France, Cybersel

Depuis plus de 25 ans, Mick accompagne de grandes organisations dans la mise en œuvre des nouvelles technologies pour améliorer leurs processus métiers. Avant de rejoindre Cybersel, il a notamment travaillé au sein de SUEZ Environnement, CGI et Digital Equipment.

Dalila BenAttia

Terranova Security

Juriste de formation, Dalila compte plus de 15 ans d'expérience dans la conduite de projets de formation continue et de E-learning en sécurité de l'information, notamment auprès de l'université Paris Descartes, Veritas Software et Symantec. Passionnée de nouvelles technologies et de digital learning, l'écoute des besoins de ses interlocuteurs est une préoccupation permanente pour elle.

Amina Bouras

Directrice de la Protection des données, Groupe PRO BTP

Amina a démarré sa carrière dans la recherche scientifique, et plus particulièrement sur la fiabilité et l'optimisation des algorithmes. Elle a ensuite rejoint le monde de l'assurance, où elle a prit les responsabilités des sujets financiers et actuariels pendant plus de 15 ans.

Aujourd'hui en charge de la gouvernance des données au sein du groupe PRO BTP (groupe de protection sociale) elle couvre les aspect organisation, qualité et valorisation de la donnée.

Yves Destrebecq

Responsable prévention contre la fraude, HSBC

Dans son poste actuel, Yves Destrebecq a mis en place et pilote le programme de prévention contre la fraude composé notamment de : – Veille, études et projets informatiques, – Evénements clients sur les thématiques fraude & cybercriminalité, – Formation & sensibilisation des collaborateurs, – Communication auprès des clients et collaborateurs, – Revue régulière et optimisation du dispositif de prévention, – Représentation de HSBC France dans certains comités interbancaires. Il travaille chez HSBC depuis 2014 et il a une expérience professionnelle de près de 20 ans réalisée au sein de différentes entreprises.

Vincent Ferran-Lacome

Architecte de la Sécurité de l'Information, L'Oréal

Vincent a commencé sa carrière à Londres pendant deux ans, d'abord chez british telecom dans leur centre de R&D sécurité, puis chez JPMorgan comme développeur. Il a ensuite participé à la création du CERT société générale, et travaillé pour la banque de France. Il a également travaillé pour BNP Paribas, dans l'équipe CSIRT, et au cours de sa dernière expérience professionnelle, il était architecte sécurité chez Euronext, avant de rejoindre L'Or al, dans le même rôle. Vincent travaille notamment sur des problématiques sécurité liées au cloud.

Hervé Fortin

Responsable de la Protection des données & RSSI Adjoint, Laboratoires Servier

Avec plus de 20 ans d'expérience dans le monde informatique et 15 ans dans la vie privée, Hervé a travaillé comme CISO et DPO pour une collectivité territoriale puis dans l'industrie pharmaceutique. Hervé couvre tous les aspects de la sécurité et de la protection de la vie privée, qu'ils soient techniques, juridiques, organisationnels ou de gouvernance.

Gaëtan Gesret

Southern Europe Solutions Engineer, Proofpoint

Membre de l'équipe d'experts Proofpoint depuis 2017, Gaëtan a effectué une partie de son parcours à l'étranger, travaillant sur un large périmètre clients dans toute l'Europe. Il se concentre dorénavant sur la protection des grandes organisations Françaises. Gaëtan a développé une parfaite maîtrise des solutions Proofpoint dédiées à la protection contre les menaces cyber (sécurisation avancée de la messagerie et des applications IaaS/SaaS, prévention et gestion des menaces internes, automatisation de la réponse sur incident). Gaëtan évolue depuis plusieurs années dans le domaine de la sécurité informatique. Il a notamment travaillé 4 ans comme consultant senior et responsable technique au sein d'un « pure player » français. A travers une large variété de missions menées avec succès pour ses clients, Gaëtan a contribué à la sécurisation d'infrastructures IT complexes et à l'optimisation des opérations de sécurité. Au début de sa carrière, Gaëtan a travaillé en tant qu'ingénieur au sein de la cellule CERT/CSIRT d'un opérateur d'importance vitale (OIV), contribuant au quotidien à la gestion des incidents de sécurité, à la veille sécurité logicielle, aux activités de vulnerability & patch management, ou encore à l'intégration de la sécurité dans les projets de transformation digitale. Gaëtan est diplômé en Ingénierie des Systèmes d'Information et de la Communication de l'Institut Mines-Telecom Lille-Douai.

Ekbal Gharbi

Sales Engineer, Cofense

Ekbal Gharbi est une ingénieure commerciale expérimenté avec 10 ans d'experience dans l'industrie informatique. Possédant un diplôme d'ingénieur en télécommunications, Ekbal a travaille en tant que consultante technique dans différentes sociétés multinationals. Ekbal a rejoint Cofense en 2017a Dubai, Émirats Arabes Unis pour faire partie de l'équipe META et aider la région à unir l'humanite contre les attaques de phishing.

Valentin Jangwa

Regional Sales Director, Southern Region, Bitglass

Valentin has been working in various sales positions in the security industry for more than 20 years, with extensive experience in various IT security fields. In his current role as Regional Director at Bitglass, he interacts with customers to discuss their cloud strategies on security. Valentin frequently speaks on security issues at various conferences across the region and is working hard with our customers as a trusted advisor in order to facilitate them with securing our customer's cloud applications and networks.

Guilhem Labourel

Account Executive, Darktrace

Yvan Lanzada

Ingénieur technico-commercial, Hermitage Solutions

Depuis plus de vingt ans, Yvan accompagne les revendeurs, intégrateurs informatiques et MSPs dans le choix et la mise en oeuvre de solutions de cybersécurité. Il coordonne de nombreux projets allant de la sécurité périmétrique, des données, des utilisateurs, à la protection des infrastructures, jusqu'aux projets d'audit de conformité et de respect des normes. Avant de rejoindre Hermitage Solutions, il a travaillé pour différents éditeurs informatiques et distributeurs de solutions de cybersécurité.

Christophe Leautey

Regional Sales Director, BitSight

Depuis plus de 20 ans Christophe aide les entreprises Fortune 500 à réduire leurs risques Business et IT grâce aux nouvelles technologies et à l'analyse des données. Avant BitSight il a travaillé au sein d'éditeurs tels que Splunk, SAS Institute ou Remedy (aujourd'hui BMC Software).

Nicolas Liard

Solutions Engineer, Bitglass

Nicolas has held various technical and commercial positions, and has been well known as a trusted advisor in the cybersecurity industry for over 15 years. In his current role as Solutions Engineer at Bitglass, Nicolas brings his technical expertise in cloud security to assist

organisations with their digital transformation and remote workforce challenges. Nicolas is also AWS and Ethical Hacking certified.

Thomas Limpens

Solution Engineer South-West-Europe, Netwrix

Thomas a plusieurs années d'expérience en tant qu'ingénieur des systèmes d'information. Il a aidé les organisations à protéger leurs infrastructures informatiques, optimiser leurs procédures et à répondre aux audits de conformité.

Arnaud Martin

RSSI,
Caisse des Dépôts

Après une double formation franco-allemande d'ingénieur, mon parcours diversifié au sein du groupe Orange (cinq années dans l'informatique, cinq années dans le réseau et six années dans la sécurité) m'a permis d'acquérir une vision globale des enjeux stratégiques et ruptures technologiques actuelles chez un opérateur telecom international. Au-delà de la composante « manager d'équipes opérationnelles » qui constitue le fil conducteur de ma carrière, j'ai également développé une dimension business importante à Orange Business Services.

Hugues Masselin

Bug Bounty Specialist,
HackerOne

Hugues accompagne les entreprises en France et au Benelux à construire des programmes performants et sur-mesure de "Sécurité Collaborative" tels que les programmes de Divulgation Coordonnée de Vulnérabilités ou de Bug Bounty. Il évolue dans l'industrie de l'IT depuis 6 ans au sein de sociétés comme SAP et vient d'ouvrir mi-2019 les bureaux de HackerOne à Paris. Ses relations avec la communauté française et internationale de hackers éthiques, l'amène à créer des ponts entre cette communauté et leurs homologues en entreprise. En dehors de HackerOne, Hugues affectionne le triathlon de longue distance et contribue notamment au développement de "ReminiSens" une expérience de voyage dans le temps à Versailles.

Xavier Mell

Country Manager France,
French speaking Africa, Pulse Secure

For more than 15 years, Xavier has supportsed companies in securing their IT environments. With a technical background, Xavier started his carreer with a leading integration for security solutions. Ever since, he has continued to build expertise on providing the best in class security solutions to companies. Xavier joined Pulse Secure in 2005 and was one of the first members of the South Europe team. He became Country Director in 2019.

Vincent Meysonnet

Senior Sales Engineer,
Cybereason

Vincent Meysonnet joined the Cybereason team in 2020 as a Senior Sales Engineer. He has 15 years' experience in IT and security companies and held pre-sales roles with software providers such as Ruckus wireless, Aastra Mitel, Ucopia, Trend Micro and Bitdefender. After that, he created and managed several pre-sales teams as well as press relations as an SE Manager and Content Specialist.

Joel Mollo

Regional Director, South EMEA,
CrowdStrike

Oren Nadjar

CTO, Groupe français indépendant de cosmétiques de luxe

Oren Nadjar est le directeur technique d'une marque de beauté française dédiée aux soins de la peau, au maquillage et aux parfums. À ce titre, il supervise l'architecture et la transformation du Cloud, la gestion et l'intégration des données, et les systèmes et réseaux. Auparavant, il a été directeur technique au SMCP (Sandro, Maje, Claudie Pierlot) d'avril 2017 à août 2018. Avant de rejoindre le SMCP, M. Oren a été directeur technique du Groupe Chantelle pendant près de deux ans et directeur technique de Zodiac Pool Systems (2013–2015).

Willem Peerbolte

Group CISO,
ODDO-BHF

Willem Peerbolte est RSSI Groupe chez ODDO-BHF, 1er groupe financier Franco-Allemand indépendant. Willem a plus de 15 ans d'expérience dans la cyber-sécurité. Il a notamment travaillé durant plus de 10 ans pour BNP Paribas. Tout d'abord en tant que RSSI chez Arval, puis chez CIB-GECD, et enfin au siège, en tant que Directeur de programme transformation cyber sécurité pour tout le groupe BNP Paribas. A ses moments perdus, Willem fait tourner son atelier de modélisation et d'impression 3D.

Frederik Rouleau

Architecte de Solutions,
TLScontact

Tom Sams

Solutions Engineer,
Digital Shadows

Tom est ingénieur en solution spécialiste en sécurité ayant comme spécialité la Sécurité Applicative, la Threat Intelligence et la Réponse aux Incidents de Sécurité, plus particulièrement au sein du secteur privé et de la défense (UK). Maitrise technique et connaissances approfondis des sujets suivants: SIEM, SIO (Security Intelligence and Operations), Threat Intelligence, Application Security (SAST, DAST).]

Federico Smith

Cybersecurity Expert, Octopus Cybercrime Community,
Council of Europe

Expert en cybercriminalité et cybersécurité, Federico a participé dans le conseil de nouvelles technologies, la dénomination dans le cyberespace, le financement de la recherche et du développement, la protection de la propriété intellectuelle sur Internet et la cybersécurité. Depuis 2011, en tant que hacker éthique, il est impliqué dans la coopération contre la cybercriminalité au sein de la communauté Octopus Cybercrime du Conseil de l'Europe. Il collabore avec plusieurs organisations internationales pour analyser et réfléchir sur les questions juridiques, la cybersécurité, la dénomination dans le cyberespace au sein de l'ICT (International Cyber Threat Task Force) et de l'IACP (International Association of Cybercrime Prevention) et en tant que trésorier membre d'Eurolinc (ONG), et plus récemment en tant qu'expert en cybersécurité dans le cadre de projets de recherche et développement de la Commission européenne (H2020) et pour l'Agence européenne de défense, et formateur en cybersécurité auprès de différents États membres en Europe.

Andy Spencer

VP Sales Engineering,
Cofense

Andy Spencer a 25 ans d'expérience en informatique, depuis ses débuts en tant que gestionnaire de systèmes et consultant jusqu'à son poste actuel de Vice-Président chez Cofense en charge des Ingénieurs des Ventes. Au cours de ses nombreuses années chez Veritas et Symantec, il a acquis une expérience non négligeable dans le stockage et la sécurité des données. Son objectif principal a toujours été d'améliorer les résultats commerciaux de ses clients grâce à des solutions informatiques innovantes. Andy a travaillé avec succès avec des agences gouvernementales et des entreprises du Global 1000 dans de nombreux secteurs, en les aidant à aligner les fonctionnalités informatiques avec leurs objectifs organisationnels. Il a la vision que les utilisateurs devraient être le lien instinctif dans le réseau de cyberdéfense, car ils ne sont pas le point le plus faible. Il s'engage donc passionnément à faire participer le facteur humain à la sécurité informatique.

Paul Steiner

Responsable conformité SI,
La Française des Jeux

Après plusieurs années dans le secteur industriel de la fabrication de cartes à puce, Paul a consolidé une expérience diversifiée en sécurité de l'information grâce aux postes de Chef de projets sécurité de solution IT, d'Auditeur pour un système de gestion en sécurité centralisée et de Responsable conformité de solutions cryptographiques embarquées. En 2008, il a rejoint le groupe FDJ (Française des Jeux), la 4e loterie mondiale et la 2e loterie européenne, afin de piloter et de garantir la conformité de différents référentiels.

Jan Tietze

Director Security Strategy EMEA,
SentinelOne

Before joining SentinelOne in 2020, Jan Tietze served in senior technical and management roles ranging from engineering to CIO and CTO roles for global IT and consultancy organisations. With a strong background in enterprise IT and an early career in senior field engineering roles in Microsoft and other security and consulting organisations, Jan understands real world risk, challenges and solutions and has been a trusted advisor to his clients for many years.

Theo Zafirakos

CISO Coach and Professional Services, Security Awareness Speaker, Terranova Security

Theo est un leader de la sécurité expérimenté, un conseiller de confiance et un expert en stratégies de sensibilisation à la sécurité, de la gouvernance, de la confidentialité et de la cybersécurité. Il collabore avec des responsables de la sécurité du monde entier pour les aider à identifier, évaluer et gérer les risques liés à la sensibilisation à la sécurité. Theo dirige également l'équipe des services professionnels de Terranova Security, qui aide les clients à mettre en œuvre et à exécuter des programmes de sensibilisation à la sécurité qui génèrent des résultats mesurables. Il veille à ce que

tous les programmes contribuent à la réalisation des objectifs de sensibilisation à la sécurité d'entreprise des clients en s'appuyant sur les 5 étapes de sensibilisation à la sécurité. Avant de se joindre à Terranova Security, Theo a passé 20 ans chez Canadian National Railway (CN). En tant que RSSI, il était responsable de la stratégie de sécurité et de gouvernance de l'information. Il a également dirigé l'unité de la sécurité des informations de l'entreprise, où son mandat était de s'assurer que le programme et les contrôles de sécurité appropriés étaient en place et appliqués dans l'ensemble de l'organisation. Theo a dirigé un programme de prévention et de sensibilisation à la cybersécurité visant à protéger le CN de toutes les cybermenaces. □

Cybervigilance et télétravail: Protégez-vous contre les cybermenaces

Cette précipitation à envoyer les employés travailler de la maison a révélé plusieurs failles de sécurité et a ouvert toute grande la porte aux fraudeurs.

Par Terranova Security

La COVID-19 a rapidement redéfini les façons dont nous travaillons, communiquons et interagissons entre nous. Des entreprises privées, des institutions publiques et des ministères exigent que tous leurs employés qui le peuvent travaillent de la maison.

Les employeurs ont eu très peu de temps pour préparer leurs employés au télétravail. Cette précipitation à envoyer les employés travailler de la maison a révélé plusieurs failles de sécurité et a ouvert toute grande la porte aux fraudeurs.

Les cybercriminels savent que les employeurs n'ont pas eu le temps de former leurs employés sur les bonnes pratiques de sécurité en télétravail ou de s'assurer que les logiciels, correctifs de sécurité et systèmes d'exploitation sont à jour sur l'ensemble des ordinateurs portables.

Comment assurer sa cybersécurité en télétravail

Au travail, la sensibilisation à la cybersécurité fait partie des priorités. Toutefois, lorsque les gens changent leurs routines de travail, leurs habitudes de cybersécurité peuvent également changer.

Pour demeurer en cybersécurité tandis qu'ils travaillent à distance, les employés peuvent suivre les directives suivantes :

- Utiliser une connexion sécurisée pour accéder au réseau de l'entreprise. S'assurer que le VPN de l'entreprise est configuré pour une authentification multifacteur.
- Travailler uniquement de la maison et ne pas se connecter au réseau de l'entreprise à partir d'un accès Wi-Fi public non sécurisé.
- Ne pas partager des données et des informations liées au travail avec les appareils personnels. Il existe un risque que ces appareils n'aient pas les mises à jour et n'utilisent pas les systèmes d'exploitation et les navigateurs les plus récents.
- S'assurer que les applications, systèmes d'exploitation, outils réseau et logiciels internes installés sur votre ordinateur ont été mis à jour.
- Créer de nouveaux mots de passe solides pour votre ordinateur portable, vos appareils mobiles et votre courrier électronique.
- Évitez de conserver ou d'imprimer des documents papier contenant des informations sensibles chez eux.

Phishing et fraudes sur les médias sociaux – comment se protéger

En raison du contexte actuel, les cybercriminels se font passer pour des ministères et des autorités de la santé. Ils envoient des courriels et publient sur les médias sociaux en espérant exploiter les craintes et les questions sans réponses que suscite le nouveau coronavirus.

Adoptez ces habitudes de sensibilisation à la cybersécurité pour vous protéger contre le phishing et les autres cybermenaces :

- Si vous ne reconnaissez pas l'expéditeur d'un courriel, ne l'ouvrez pas.
- Portez une attention particulière à l'orthographe des adresses de courrier électronique, des lignes d'objet et du contenu des courriels.
- Méfiez-vous des courriels qui utilisent un ton urgent et vous demandent de les aider en transférant des fonds ou en partageant de l'information confidentielle.
- Ne cliquez pas sur des liens compris dans des courriels non sollicités.
- Ne partagez jamais des informations confidentielles par courriel.
- Lorsque vous magasinez en ligne, inspectez toujours la barre d'adresse et vérifiez que l'URL contient «https» ou l'icône du cadenas.
- Sur les médias sociaux, n'acceptez pas des abonnés ou des amis que vous ne reconnaissez pas. Si un compte auquel vous ne faites pas confiance vous fait une demande d'abonnement ou d'amitié, bloquez ce compte.
- Si vous n'êtes pas certain de la validité d'un courriel ou d'un autre message, ne répondez pas. Si vous recevez un courriel étrange de la part d'un collègue ou d'un patron, validez l'information avec cette personne de vive voix.

Rappelez à vos employés que les meilleures pratiques de sensibilisation à la sécurité et de cybersécurité s'appliquent partout – au bureau, à la maison, dans l'autobus, à l'aéroport, au café – dès le moment où ils se connectent à Internet Télécharger ma trousse de cybersécurité pour le télétravail. □

Pour plus d'informations : **terranovasecurity.com**

TERRANOVA SECURITY

TERRANOVA SECURITY

SENSIBILISATION À LA CYBERSÉCURITÉ CENTRÉE SUR LES PERSONNES

- Simulations de phishing basées sur des cas réels
- Contenu interactif disponible en 40 langues
- Modules d'apprentissage en format e-learning, microlearning et nanolearning

Réduisez les risques et impacts des cyber attaques en créant une première ligne de défense avec votre propre équipe de cyber héros.

TERRANOVASECURITY.COM/FR-FR

Solving the security challenges of remote working

For some, the switch to remote working has been quick and painless, but for many others, a lack of advanced planning has made it a significant challenge.

By Bitglass

Unprecedented times call for unprecedented actions has caused what is likely to be the biggest shift towards remote working that the world has ever seen. However, while the technology has been around for quite some time, recent events demonstrate just how few businesses can switch from an office-based setup to a remote one in a fast, secure, and non-disruptive manner.

There's a significant number of reasons why it is prudent to have a remote working infrastructure in place. Truth be said, 'in the event of a global pandemic' probably wasn't very high up most people's list before 2020. In normal circumstances, common occurrences like adverse weather, transportation issues, and power outages can also severely affect the productivity of business if employees can't access what they need outside the office. The right security tools must be in place, otherwise, businesses risk exposing themselves to a wide range of cyber-threats. This article will examine some of the major considerations for any business looking to implement a remote working programme that will enable employees to work both securely and effectively from anywhere.

Finding the right approach is key

Historically, office-based businesses have managed off-site workers through the use VPNs and MDM approach. While still a relatively popular strategy today, it raises an increasing number of privacy concerns, mainly because it gives businesses the ability to monitor everything employees do on their device. VPN technology is also widely considered to be outdated and its complexity means skilled IT professionals are required to manage/maintain it properly.

For businesses without legacy technology to consider, a BYOD approach is often preferable. Not only does it reduce IT costs, but employees will always be able to work on their device in the event of unforeseen circumstances. Unlike a managed device approach, employees using their own personal devices have more freedom over what and where they can view or download sensitive data, making robust security even more critical. Below are three security technologies that can be used to complement the flexibility a BYOD programme provides:

1. Data loss prevention technology keeps businesses in control

One of the biggest issues with a BYOD approach is how to prevent sensitive data loss or theft from unmanaged devices. The use of data loss prevention (DLP) technology can significantly mitigate this, giving businesses much more control over their data than they would otherwise have. With DLP in place, any unauthorised attempts to access, copy or share sensitive information – whether intentional or not – will be prevented helping to prevent security breaches.

2. Behavioural analytics quickly detects suspicious user activity

Implementation of user and entity behaviour analytics (UEBA), is a great way to quickly detect anomalous behaviour that might indicate a potential security breach. UEBA works by learning and establishing benchmarks for normal user behaviour and then alerting security teams to any activity that deviates from that.

3. Agentless technology delivers robust security without breaching privacy

Employees using personal devices as part of a BYOD programme can often be resistant to agent-based security tools being installed on them. Not only are some – like MDM – considered an invasion of privacy, but they can also impact device performance and functionality. Conversely, agentless security tools utilise cloud technology, meaning they require no installation but still give security teams the control they need to monitor, track and even wipe sensitive data if/when necessary. Furthermore, because agentless security tools only monitor company data on the device, employees can be confident that their personal data and activity remain completely private. Leading agentless security solutions even include cloud-based DLP as part of their offering, meaning businesses can cover multiple bases in one go.

Over the last few months many businesses has been forced to fundamentally change the way they operate. For some, this switch to remote working has been quick and painless, but for many others, a lack of advanced planning has made it a significant challenge. By combining BYOD with powerful cloud security and analytics technology, businesses can quickly establish an effective, secure remote working programme, keeping the wheels of business turning. □

For more information, please visit
www.bitglass.com
bitglass

bitglass

Security for any app, any device, anywhere.

Secure mobile device access

Data loss prevention

Compliance

User and entity behaviour analytics and cross-app visibility

Comment BitSight prend-il en compte les nouveaux cyber-risques induits par le Work From Home?

En 2011, BitSight, a été le pionnier du marché des notations de sécurité en se donnant pour mission de transformer la manière dont les entreprises évaluent les performances en matière de risque et de sécurité sur la base du modèle de référence utilisé par les agences de notation.

Par BitSight

BitSight fournit une visibilité à partir d'observations faites depuis l'extérieur du réseau de l'entreprise : c'est la vision que pourrait avoir un cyber-attaquant cherchant à identifier des cibles d'opérations malveillantes.

Cas d'usage BitSight

BitSight fournit une mesure continue de la posture de cyber sécurité de n'importe quelle société afin d'en évaluer les cyber-risques et de mener, en fonction des ressources disponibles, les actions de remédiation permettant la réduction de ces risques.
BitSight est utilisé par les équipes de sécurité, de gestion des risques, d'audit et de contrôle interne pour :

- Mesurer les performances de de sécurité de l'entreprise au niveau du groupe et de chacune des entités légales ou organisationnelles afin de :
  - Apporter une visibilité aux équipes de réponse a incidents et à celles en charge de l'hygiène de sécurité sur les compromissions en cours ainsi que sur les principales menaces qui pèsent sur l'entreprise
  - Prioriser les actions de remédiation en fonction des ressources disponibles
  - Comparer les performances de sécurité de mes filiales et entités organisationnelles (business units, départements, …) et identifier les impacts de chacune d'entre elles sur les risques portés par mon groupe.
  - Comparer les performances de l'entreprise avec celle de ses pairs et des indices standard de son secteur d'activité
  - Fournir aux différentes parties prenantes de l'entreprise des tableaux de bord sur la posture de sécurité de l'entreprise et les cyber- risques les plus prégnants.
  - Analyser ma surface d'attaque : assets on premisses, assets dans les infrastructures cloud, filiales et entités organisationnelles, géographie, services exposés
  - S'intégrer aux solutions de sécurité opérationnelle et de gestion des risques (SIEM, SOAR, GRC, …).
- Monitorer en continu les risques afférents aux tierces parties de l'entreprise (fournisseurs, partenaires, clients) afin de :
  - Apporter une visibilité sur les principaux risques et menaces au sein de mon écosystème susceptible d'impacter mon entreprise
  - Identifier les tierces parties les plus critiques et adopter un plan de surveillance adapté : mise en place d'alertes paramétrables, déclenchement d'actions dans des outils tierces (par exemple déclenchement automatique d'envoi de questionnaire dès que les performances d'un fournisseur baissent),
  - Surveiller les fournisseurs tout au long de leur cycle de vie (de l'appel d'offres à la fin des relations) et selon leur catégorisation.
  - Collaborer avec leurs tierces parties sur la base de leurs performances de sécurité
  - Identifier les technologies les plus à risque pour mon entreprise au sein de mon écosystème
  - Évaluer les performances de sécurité de cibles de fusion et acquisition
  - Fournir des métriques et des tableaux de bord simples aux autres parties prenantes de l'entreprise (achat, juridique, financier).
  - S'intégrer aux autres solutions de gestion de la sécurité des tiers et de gestion des risques (Questionnaire Management, TPRM, GRC, …)

Cyber-risque et télétravail

Une récente étude menée par BitSight auprès de 41 000 organisations a montré que près de la moitié des devices qui accèdent à leur réseau dans le cadre du télétravail de leurs salariés sont infectés par au moins un malware. Les hackers ont d'ailleurs intensifié leurs activités afin de profiter de cette situation et d'exploiter les nouvelles failles et vulnérabilités auxquelles les utilisateurs sont désormais exposés (accès wifi exposés, interfaces d'administration des routeurs paramétrés avec des mots de passe par défaut, rootkit sur les clients Citrix, …).

Afin d'aider les équipes de sécurité à identifier et à gérer ces nouveaux risques, BitSight a intégré la solution BitSight Work From Home – Remote Office permettant de :

- Identifier les vulnérabilités et les infections sur les adresses IP connues et les traiter dans le cadre de leur processus de réponse à incidents.
- Surveiller et gérer les environnements d'exploitation à distance à haut risque, tels que les compte à privilège ou les utilisateurs ayant accès à des données sensibles
- Sensibiliser les utilisateurs à ces nouveaux risques et leur diffuser les bonnes pratiques de sécurité dans le cadre du télétravail. □

Pour plus d'informations :
www.bitsight.com

BITSIGHT®
The Standard in SECURITY RATINGS

Identifier et mesurer simplement vos cyber risques.

Les notations de sécurité Bitsight pour évaluer vos performances de sécurité et celles de votre Eco-système

Augmentez la fiabilité des Evaluations de Cyber risques.

Analysez votre nouvelle surface d'attaque.

Mesurez en continu la sécurité de vos tierces parties.

+2000 organisations dans le monde utilisent déjà les notations de sécurité Bitsight.

Et vous ?

Cybersel

BITSIGHT®
The Standard in SECURITY RATINGS

www.bitsighttech.com

Réduisez les risques de sécurité

Les entreprises mondiales, les start-ups et les organismes gouvernementaux se tournent vers les tests de sécurité collaboratifs.

Par Synack

Depuis le premier jour, nous avions un objectif simple : fournir une solution de sécurité évolutive, capable d'aider les organisations modernes à minimiser les risques de sécurité.

Les tests d'intrusion traditionnels ressemblent à la procédure des listes noires pour bloquer le spam : insuffisants et obsolètes. Les tests d'intrusion traditionnels sont basés sur des listes de contrôle et sur la conformité, et ne parviennent pas à imiter la créativité de l'adversaire. Généralement, ces tests sont effectués par de petites équipes statiques qui n'arrivent pas à maîtriser l'étendue des surfaces d'attaque modernes et la diversité des attaquants. Avec un déficit de talents qui devrait atteindre 3,5 millions de postes ouverts en cybersécurité d'ici quelques années (Cybersecurity Ventures), des mises à jour rapides et avec des systèmes d'alerte bruyants, il n'est pas étonnant que les équipes de sécurité cherchent une réponse plus efficace et plus pertinente pour trouver et corriger les vulnérabilités. C'est pourquoi les entreprises mondiales, les start-ups et les organismes gouvernementaux se tournent vers les tests de sécurité collaboratifs.

Cette approche moderne en test d'intrusion offre une ampleur, une efficacité et une pertinence inédites. Cependant, les entreprises de sécurité en testing collaboratif ne sont pas toutes identiques. Les solutions de tests collaboratifs varient en fonction de la qualité et de la confiance que l'on peut accorder, du contrôle dont dispose le client, de la gestion et de la technologie d'analyse sophistiquées, de la rapidité et de la simplicité du déploiement, et du niveau de service d'assistance axé sur la découverte, le tri, le reporting et la remédiation aux vulnérabiltés, autant de facteurs entraînant un retour sur investissement différent.

Synack est la plateforme sécurité de test collaboratif pour les F500/G2000, le marché intermédiaire et les organismes gouvernementaux conçue spécialement pour la confiance, le contrôle et la visibilité. Comme les tests d'intrusion traditionnels, Synack exploite le meilleur de l'intelligence humaine et artificielle - mais pas seulement un groupe de testeurs et un algorithme générique. Synack associe cette puissante combinaison de talents humains et de technologie avec des données et la visibilité pour un service en profondeur, rigoureux et constant 365 jours par an. Voici la recette du succès de notre plateforme :

1. *L'intelligence humaine – Synack Red Team :* Les meilleurs chercheurs du monde, contrôlés pour leurs compétences et leur fiabilité et récompensés en fonction de ce qu'ils trouvent, plutôt que du nombre de cases qu'ils cochent
2. *L'intelligence machine – la plateforme de Synack :* La plateforme d'intelligence machine de Synack est renforcée par les enseignements apportés par la Synack Red Team et permet d'accélérer la détection de vulnérabilités.
3. *Les renseignemens et la visibilité – LaunchPoint :* une passerelle sécurisée pour toutes les activités de test qui offre une réduction des risques aux clients et aux chercheurs, un contrôle clients et des analyses en temps reel
4. *"Service de conciergerie" – Synack Operations :* Un multiplicateur de force qui fait ce que vos équipes ne devraient pas avoir à faire, notamment des déploiements rapides, la gestion de programmes 24 heures sur 24 et 7 jours sur 7, la suppression du bruit par le tri et la vérification des correctifs, le suivi en continu des performances et la gestion communautaire

Les quatre composantes de notre plateforme fonctionnent ensemble pour fournir une solution simple, compréhensible et efficace avec des analyses en temps réel et des rapports détaillés à la demande. Une façon simple de comprendre votre risque de sécurité du point de vue d'un véritable hacker.

Un test d'intrusion Synack signifie :

- *Valeur plus élevée Le retour sur investissement :* 4x plus élevé qu'avec les méthodes traditionnelles grâce aux gains d'efficience obtenus par l'automatisation, la réduction du bruit et des connaissances plus exploitables
- *Une plus grande efficacité La plateforme intelligente :* de Synack réduit 99,8 % du bruit, ce qui permet aux chercheurs de concentrer leurs efforts sur les vulnérabilités les plus critiques et les plus exploitables
- *De meilleurs résultats :* Une résistance accrue de 200 % aux attaques malveillantes grâce à une cadence continue de tests humains + machine et à une couverture continue des applications dynamiques

Qu'est-ce que cela donne finalement ? Une compréhension réaliste des risques de sécurité et des résultats exploitables. □

Pour plus d'informations, visitez notre site **www.synack.com**

Synack

Synack®

L'ARME ULTIME DE LA CYBERSÉCURITÉ

DES TESTS D'INTRUSION EXHAUSTIFS AVEC DES RÉSULTATS EXPLOITABLES

Une sécurité continue renforcée par les chercheurs les plus compétents au monde et par l'IA

L'ENGAGEMENT DE SYNACK

La confiance se gagne, et notre devise est la droiture:

Un engagement à protéger nos clients et leurs clients.

Une totale confidentialité. Un anonymat possible. Un contrôle total du processus.

Une confiance totale lorsque vous devez vous concentrer sur votre cœur de métier.

Nous sommes Synack, la plateforme sécurité collaborative de confiance.

VISITEZ LE SITE WWW.SYNACK.COM

Comment élaborer une la lutte contre les places de marché du Dark Web

Dans notre rapport sur le Dark Web, *Seize and Desist: The State of Cybercrime in the Post-AlphaBay and Hansa Age*, nous avons étudié l'impact de ces fermetures de places de marché du Dark Web.

Par Digital Shadows

En juillet 2017, l'opération policière Bayonet menée conjointement par les États-Unis et les Pays-Bas a permis de saisir et de démanteler deux des principales places de marché du Dark Web, AlphaBay et Hansa. Le procureur général américain Jeff Sessions décrit l'opération en ces termes :

« Il s'agit de l'une des plus importantes enquêtes criminelles de l'année (…) grâce à cette opération, le peuple américain est mieux protégé contre la menace des usurpations d'identité et des malwares, et contre les drogues dangereuses. »

Avant l'opération Bayonet, l'activité cybercriminelle anglophone reposait principalement sur des places de marché du Dark Web, comme Alpha Bay et Hansa, où des centaines de milliers de vendeurs et d'acheteurs se livraient à des transactions illégales, pour une valeur estimée à plus d'un milliard de dollars.

D'autres opérations policières ont suivi. Le 7 mai 2019, une opération coordonnée au niveau international a donné lieu au démantèlement de deux autres places de marché du Dark Web : Wall Street Marketplace et Valhalla Marketplace (Silkkitie). Cette même opération a également permis de fermer l'une des sources d'informations et portes d'entrée les plus populaires du Dark Web, DeepDotWeb. DeepDotWeb ne vendait pas de produits de contrebande ; en revanche, ses administrateurs s'enrichissaient en faisant la promotion de sites et places de marché criminels par le biais de liens d'affiliation. Ce récent démantèlement témoigne de la volonté des autorités policières de cibler les réseaux de commerce illégal au-delà des places de marché, en incluant les promoteurs et les blanchisseurs

Dans notre rapport sur le Dark Web, *Seize and Desist: The State of Cybercrime in the Post-AlphaBay and Hansa Age*, nous avons étudié l'impact de ces fermetures de places de marché du Dark Web. Même si une grande partie de la cybercriminalité (russophone notamment) a été peu perturbée, la confiance dans les marchés du Dark Web a été ébranlée.

Des marchés, comme Apollon et Empire, sans doute encore actifs, n'ont pas encore atteint la puissance de Silk Road, AlphaBay ou Hansa. Si de nouvelles places de marché illégales apparaissent en permanence, elles ont plus en plus de mal à se développer ou se font plus prudentes, eu égard à la menace croissante des fermetures et démantèlements par les forces de l'ordre. Pour prospérer, ces places de marché criminelles ont besoin d'une solide réputation, d'un financement pour évoluer, de sécurité pour fidéliser leurs utilisateurs et de confiance pour recueillir une plus large adhésion.

Market.ms en est un bon exemple. Cette place de marché était gérée par l'ancien administrateur de la prestigieuse plateforme de piratage Exploit[.]in et étoile montante du marché du Dark Web, qui cela dit en passant dirige désormais la nouvelle plateforme XSS (anciennement, Damagelab). Exclusivement spécialisé en cybercriminalité, MarketMS était presque sans égal. Et pourtant, cette crédibilité n'a pas permis à MarketMS de générer le chiffre d'affaires nécessaire pour assurer sa viabilité.

Les cybercriminels ne s'en remettent pas à un seul site, mais sont présents sur nombre de ces sources afin de se faire connaître aux acheteurs potentiels. L'offre de services de dépôt de garantie constitue un attrait important de ces plateformes. Il est donc important de noter que ces nouveaux marchés du Dark Web coexistent avec Telegram et Jabber pour obtenir des démonstrations, négocier et convenir d'un prix final.

Accédez à l'article complet sur le Blog ici:
https://www.digitalshadows.com/fr/blog-and-research/surveillance-du-dark-web-af-le-bon-la-brute-et-le-truand/ □

Digital Shadows réduit les risques numériques en identifiant les expositions indésirables et en protégeant contre les menaces externes. Lorsque les risques numériques ne sont pas adressés, une entreprise peut faire face à des amendes pour non-conformité, une atteinte à sa réputation, ou encore à des pertes de propriété intellectuelle. La plateforme SearchLight de Digital Shadows vous aide à réduire ces risques en détectant vos pertes de données, en sécurisant votre présence en ligne et en réduisant votre surface d'attaque.

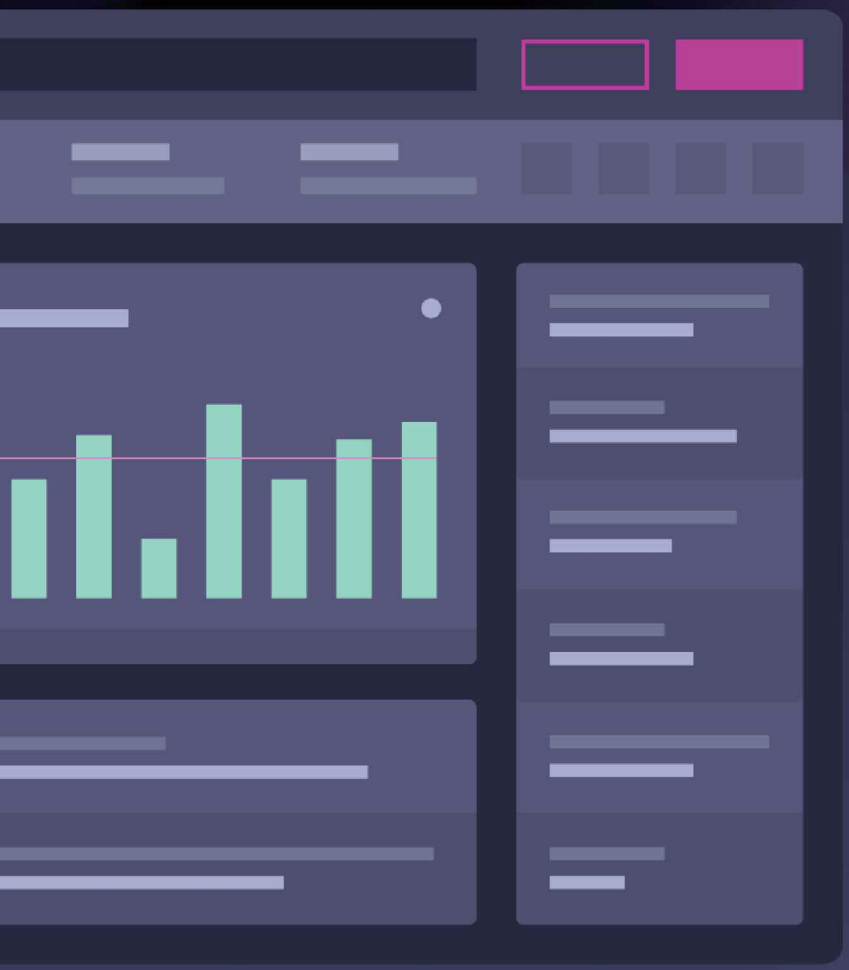
Pour plus d'informations :
www.digitalshadows.com

digital shadows_

digital shadows_

N'AIDEZ PLUS LES CYBERCRIMINELS

Avec SearchLight™, prenez le contrôle de votre empreinte numérique et éloigner les menaces en ligne.



Découvrez comment nous aidons des centaines d'entreprises à réduire leurs risques numériques via :

- Détection de pertes de données
- Protection de la Marque
- Méthodologie DevSecOps
- Surveillance du Dark Web
- Réduction de la Surface d'Attaque
- Threat Intelligence

Essayez SearchLight par vous-même !
Testez gratuitement la solution pendant 7 jours ici **www.digitalshadows.com/fr**.

Nouvelle décennie, nouvelle surface d'attaque, mêmes fondamentaux

Alors que le changement poursuit sa marche inexorable, les surfaces d'attaque, elles, n'ont jamais été aussi difficiles à appréhender.

Par Tim Erlin

À l'heure où j'écris ces lignes, l'explosion du télétravail donne d'ailleurs toute sa force à mon propos. Cette tendance, couplée à l'adoption du cloud et des objets IoT, nous montre à quel point les surfaces d'attaque ont changé.

Un mot d'abord sur la terminologie. Qu'entendons-nous par « surface d'attaque » ? Si un « vecteur d'attaque » constitue une porte d'entrée vers vos systèmes, réseaux ou informations, alors la « surface d'attaque » désigne la somme de tous ces vecteurs. Autrement dit, il s'agit de la surface d'exposition totale de votre entreprise : des systèmes de data center jusqu'aux portables des salariés, en passant par les applications cloud et les systèmes industriels connectés, le tout multiplié par la somme de vos environnements.

Ainsi chaque entreprise possède une surface d'attaque qui évolue au gré des modifications d'infrastructure, sans oublier le cloud et sa pléthore de services. Mais plus que le nombre ou le type, c'est aussi l'emplacement des appareils qui varie. On voit ainsi apparaître des environnements hybrides à la croisée du physique, du virtuel et du cloud privé et public. En parallèle, on assiste à la convergence des systèmes d'information (IT) et opérationnels (OT). Quant au monde du travail, il déserte toujours plus les bureaux traditionnels.

Si ces nouveaux environnements génèrent des risques et des dangers, la meilleure défense reste encore très ancrée dans les fondamentaux de la sécurité d'aujourd'hui.

Expansion des environnements : comment garder le rythme

Bien que les surfaces d'attaque aient beaucoup évolué, la plupart des compromissions d'envergure procèdent encore des mêmes vecteurs : erreurs de configuration, vulnérabilités non corrigées, mises à jour tardives ou erreurs humaines élémentaires. Les professionnels de la sécurité doivent donc s'interroger sur la manière d'étendre la protection de leur infrastructure existante à leurs nouveaux environnements. La réponse à l'expansion des surfaces d'attaques se situe moins dans la technologie elle-même que dans l'application rigoureuse de contrôles critiques : inventaires de ressources, sécurité des configurations, gestion des vulnérabilités, suivi des changements, etc.

Vous devez donc réfléchir à l'expansion de vos environnements et à ses implications sur la surface d'attaque. Aujourd'hui, le cloud représente l'un des principaux vecteurs de risque, à l'image de cet industriel qui a laissé fuiter quelque deux milliards de données, dont les informations personnelles de ses clients. Et comme toutes les données transmises par ses objets connectés étaient centralisées sur un même environnement cloud, les attaquants n'ont eu qu'à briser un seul verrou.

Tout récemment, de nombreuses structures ont basculé en télétravail dans l'urgence, avec peu ou pas de planification en termes d'impact sur leur surface d'attaque. Dans cette nouvelle configuration, les équipes de sécurité ont besoin de visibilité sur les systèmes distants des collaborateurs (niveaux de protection, vulnérabilités, conformité, etc.).

Contrôles critiques : un impératif absolu

L'apparition de nouveaux vecteurs de risques et l'expansion des surfaces d'attaque entraînent une démultiplication des outils de sécurité, elle même synonyme de complexification des environnements à protéger. Or qui dit plus de complexité dit aussi plus de risque.

On peut néanmoins briser cette spirale dès lors que les contrôles les plus fondamentaux sont appliqués systématiquement. D'où l'importance de se doter d'une stratégie de cybersécurité adaptée, d'en comprendre tous les ressorts et de plancher sur les moyens de renforcer constamment votre sécurité.

Identifier les problèmes, corriger les vulnérabilités, cibler les menaces prioritaires... en 2020, la réponse au défi de la sécurité demeure la même qu'il y a vingt ans. □

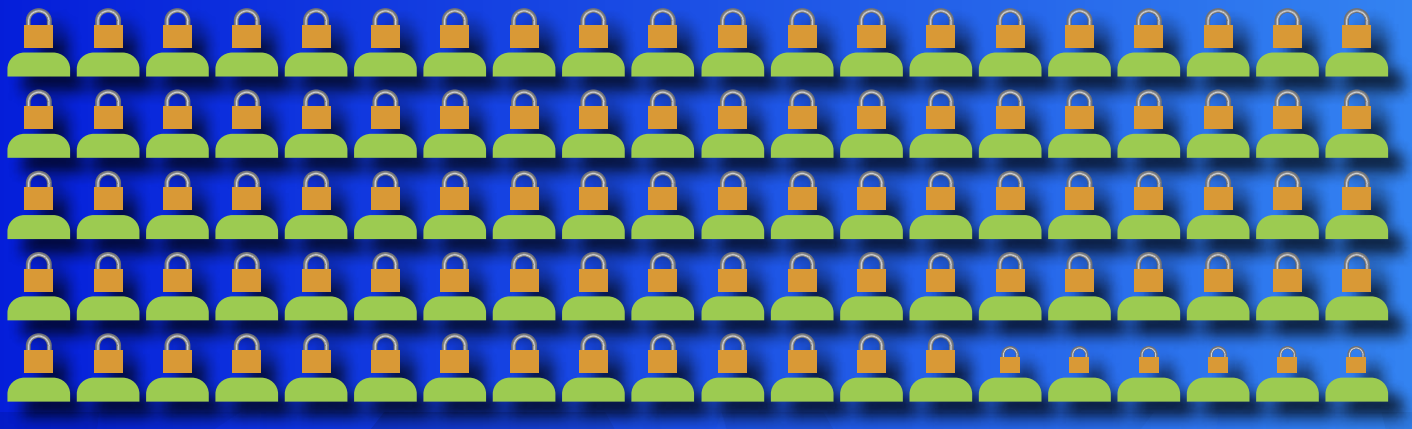
Tim Erlin, VP gestion et stratégie produit, Tripwire.

Pour plus d'information, écrivez-nous à emea_sales@tripwire.com ou appelez-nous au +44 (0)1628 775850.

www.tripwire.com

94%

des professionnels de la cybersécurité sont plus préoccupés par la sécurité aujourd'hui qu'avant le COVID-19



Obtenez le rapport d'impact du COVID-19 en matière de cybersécurité

La pandémie a servi de test de stress majeur en ce qui concerne les contrôles et politiques de sécurité. La hausse du télétravail a élargi le champs d'attaque et créé de nouveaux défis pour les équipes de sécurité.

Découvrez comment les entreprises ont réagi en sécurisant les environnements de travail à domicile de leurs employés, en connectant des appareils distants aux réseaux d'entreprise et en déjouant les cyberattaques liées au COVID-19. **tripwire.me/COVIDresearch**

Tripwire aide, depuis 20 ans, les entreprises à contrôler l'intégrité des systèmes, à automatiser la conformité réglementaire et à gérer les vulnérabilités des réseaux. Comment pouvons-nous vous aider ?

tripwire®

***The State of Security*:** Actualités, tendances et opinions en matière de sécurité sur **tripwire.com/blog**
Suivez-nous sur LinkedIn, Twitter et Facebook

©2020 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All rights reserved.

To pay or not to pay

The nuances of when it makes sense to enter into negotiations and when it makes sense to pay ransoms for hostages or not is not as straightforward as a five-word policy.

By Sam Curry

We've all seen the movie: the steely eyed law enforcement officer draws a deep breath and says firmly "we don't negotiate with terrorists. Ever." But the fact is, we do. It might be appealing to have a clear-cut, black-and-white measure for when to talk or when to shut down talks; but the nuances of when it makes sense to enter into negotiations and when it makes sense to pay ransoms for hostages or not is not as straightforward as a five-word policy.

That brings us to ransomware and whether to pay or not, and it's neither simple nor straightforward for policy makers. New York State is deliberating two bills on ransomware: S7246 introduced by Sen. Phil Boyle, (R), and S7289, introduced by Sen. David Carlucci (D). Both would make it illegal to pay ransoms, one for the government and one more generally. While the sentiment here of 'enough is enough' and taking a strong stance is important, it has to be more than virtue signalling or these laws and others like it have the potential to do real damage to the victims.

Before continuing, let's make clear the differences between ethical and legal frameworks. An ethical framework is a mechanism for determining right and wrong: religious frameworks for instance believe that right aligns with divinity while frameworks like utilitarianism believe that right aligns with the most good for the most people. This is not an endorsement of any framework, but rather an important difference to highlight because laws codify what will be encouraged or discouraged, sometimes harshly in a society; and we want to pass laws that align with the ethical framework we've chosen.

The spirit of 'never pay ransoms' seems to say crime must be stopped at all costs. The ethics here suggest crime is the ultimate evil and must be stopped. To fund the dark side is not acceptable, and we should rally not to do so in a tight, disciplined, unforgiving-of-errors manner. The problem is the 'at all costs' part of that statement. Do we really mean that?

Imagine ransomware in a nuclear power plant or in the middle of a busy day in a surgical centre... or 12 surgical centres in a state like NY. Lives are in the balance here, and we run into another ethical framework: that which promotes life and human life is the most important thing. If the law was written in a way that made it illegal to pay ransoms and too bad for a nuclear incident or 12 lives waiting for surgical data and equipment to return to functional status, would you break the law? Would the penalty make you pause, and if you decided the penalty was too much and something terrible happened, would you then face potential civil damages for your choice?

Right and wrong are not necessarily aligned with the law (for a further example, see apartheid), so I would encourage legislators to tread carefully when legislating and to understand the technology and all the cases and trade offs with extreme care. Don't rush into this one! However, let's get pragmatic here and helpful to the presumable well-meaning legislators in New York and elsewhere considering something similar now or in the future.

Guidelines for ethical consideration and for public safety are essential, which demands a weighing of ethics. At the moment, we have no laws on the books regarding payment or non-payment of ransomware demands. We can say with certainty that, generally speaking, it's right to minimise all funding to ransomware gangs, but at what point is that not true? What is the price to keep subways running, to avoid being locked out of a nuclear control system or to enable a brain surgeon to finish a delicate tumor extraction? Decide how the corner cases will be handled, set the penalties accordingly and provide the public and the courts with more than just 'thou shalt not pay ransoms'.

Laws can be written that provide exceptions and guidelines or even require an independent board to consult before payment is considered rather than an absolute moratorium on payment. Ideally, such a law will do no (or least) harm and will strangle the ransom gangs of funding, while encouraging funding for critical infrastructure and new innovation in the areas we collectively find most vital to maintain in operation. We are a society of laws and, once written, we need to respect them or overturn them within the system. We cannot afford an unethical or unjust law simply to telegraph frustration over ransomware, especially when it means that the victims of ransomware will only suffer more as a result.

If you're looking for a deeper dive on ransomware threats, check out our ransomware resources page. □

Sam Curry is Chief Security Officer at Cybereason.

For more information, please visit **www.cybereason.com**

cybereason

2020

REMOTE WORK FROM HOME CYBERSECURITY REPORT

Cybersecurity INSIDERS

Research Sponsor

Pulse Secure®

Nouveau rapport sur la cybersécurité du travail à domicile à distance

Ce Rapport sur le travail à domicile 2020, parrainé par Pulse Secure et produit par Cybersecurity Insiders, offre une perspective approfondie sur la manière dont les entreprises ont procédé à la transition des travailleurs et des ressources.

Par Pulse Secure

Les solutions d'accès sécurisé permettent aux entreprises de continuer à fonctionner en assurant la sécurité de l'informatique à distance et en connectant les personnes et les appareils au centre de données et aux applications dans le cloud, même dans les circonstances les plus imprévisibles.

Comme l'impact du coronavirus (COVID-19) s'est intensifié et est devenu une pandémie, l'Organisation mondiale de la santé a suggéré que les citoyens travaillent à domicile et évitent d'utiliser les transports publics et les environnements de bureau par précaution pour atténuer la propagation et le risque d'infection.

Au début de l'année 2020, les gouvernements et les responsables locaux du monde entier ont commencé à conseiller aux citoyens ou même exiger qu'ils restent à l'abri chez eux et cessent de se rendre sur leur lieu de travail pour toutes les entreprises sauf les plus essentielles. Les entreprises ont lancé des actions immédiates pour étendre et faciliter les capacités de travail à distance depuis le domicile (TAD).

Au-delà de l'impact potentiel sur la productivité des utilisateurs, ce changement urgent de lieu de travail et le besoin rapide de capacité pour le travail à distance ont menacé l'infrastructure informatique, la continuité des activités et la sécurité des informations.

Ce Rapport sur le travail à domicile 2020, parrainé par Pulse Secure et produit par Cybersecurity Insiders, offre une perspective approfondie sur la manière dont les entreprises ont procédé à la transition des travailleurs et des ressources, et révèle les défis, les préoccupations, les stratégies et les résultats attendus en matière de cybersécurité TAD. L'enquête, menée en mai 2020, a interrogé plus de 400 décideurs, spécialistes et entreprises de tailles diverses dans plusieurs secteurs d'activité. L'enquête a révélé que 84 % des entreprises prévoient un travail à distance plus large et permanent et près d'un tiers prévoient d'augmenter leur budget pour un accès sécurisé à court terme. □

Pour plus d'informations :
www.pulsesecure.net

Pulse Secure®

Remote WORK FROM HOME Cybersecurity

Massive WFH Acceleration Due to COVID-19

Dec 2019
<25%
WFH

May 2020
>75%
WFH

Rapid Adjustment to Acceptable Use Policy

Same security controls/policy for on-premise and remote users
78%

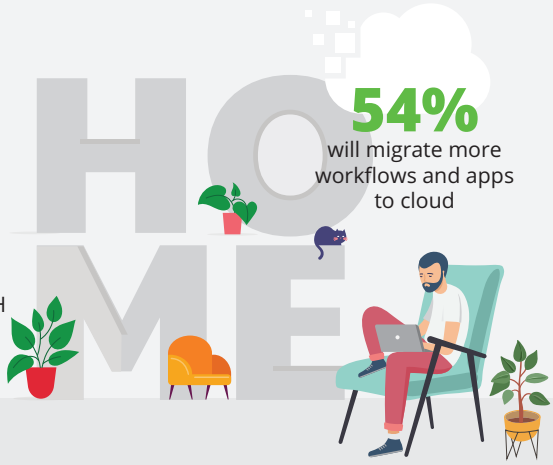
Allowing access from personal, **unmanaged devices**
65%

WFH Capacity Extending Beyond Health Crisis

38%
experienced productivity gains and other benefits

84%
anticipate broader and permanent WFH programs

54%
will migrate more workflows and apps to cloud



WFH Increase Fuels Resiliency and Security Challenges

Top 4 security challenges

- User Awareness **59%**
- Insecure Home and Public WiFI **56%**
- Use of at risk and personal devices **43%**
- Sensitive data access, leakage **41%**

Top risky WFH application exposures

- File sharing **68%**
- Web apps **47%**
- Video conferencing **45%**

33%
businesses ill-prepared or not prepared for WFH shift

69%
have strong security concerns

Greater Attack Vectors and Compliance Exposures

Top Attack Vectors

- **72%** Malware
- **67%** Phishing
- **59%** Unauthorized User, Device Access
- **44%** Unpatched System

63%
Expanded Compliance Risks

- **50%** GPDR
- **38%** PCI, DSS
- **33%** HIPAA

WFH Cybersecurity Action

55%
will continue to increase WFH / secure access budget

Top 5 WFH security solutions employed

77%	77%	66%	66%	53%
Anti-Virus/ Malware	Firewall	SSL VPN	Multi-factor Authentication	Backup

Get the complete 2020 Remote Work From Home Cybersecurity Report at **www.pulsesecure.net/WFH_cybersecurityreport/**

Source: © CyberSecure Insiders "2020 Remote Work From Home Cybersecurity Report" sponsored by Pulse Secure. survey n=412

Pulse Secure®

SentinelOne™

HUNT CYBERCRIME WITH SUPERHUMAN PRECISION.

PREVENTION | DETECTION | RESPONSE | HUNTING

Advanced Endpoint Security
Next Generation EPP
+ActiveEDR

To learn more, visit
sentinelone.com