CLUB ESSOR INNOVATION

PARIS&CO

LE PETIT GUIDE DE SURVIE AUX CYBER-ATTAQUES POUR LES PME - ETI

Réagir, Anticiper & Sécuriser

EDITO

Lancé fin 2020 par Paris&Co, le Club Essor Innovation a pour objectif d'activer l'open innovation au sein des PME / ETI du territoire francilien.

Après 10 ans de pratique de l'innovation ouverte avec les grands groupes, Paris&Co a décidé d'ouvrir son écosystème innovant, unique en France, aux PME et aux ETI qui sont les principaux acteurs de la croissance économique du territoire. Ainsi, une communauté, riche de près de 1500 startups, 100 grands comptes, 30 acteurs publics est mobilisée.

L'objectif premier du Club est d'accompagner les PME / ETI dans l'identification des solutions et innovations qui vont leur permettre d'accélérer leur développement : enrichissement de l'offre, création de nouvelles propositions de valeur, amélioration de l'expérience client et génération de nouvelles opportunités d'affaires.

Le second objectif du Club est de permettre aux PME/ETI de créer les conditions du succès de l'open innovation. En effet, les freins à la réussite de la démarche sont multiples : motivation au changement, rigidité des processus internes, maturité digitale insuffisante, perception de l'échec, etc. Le Club organise donc des actions collectives sur les volets RH, Digitalisation et RSE afin de renforcer la capacité de ses membres à intégrer l'innovation.

A ce titre, le Club s'investit sur différents sujets comme l'engagement des collaborateurs, la valorisation des données, les outils de la RSE, etc...

Les membres du Club ont donc accès à la fois à des services personnalisés de sourcing de startups ou d'experts et à une programmation collective autour des thématiques précédemment évoquées.

Les membres du Club Essor Innovation sont des PME de plus de 100 personnes ainsi que des ETI implantées en Ile-de-France, de tous secteurs d'activité.

Le contexte de la Covid 19 a imposé aux entreprises un recours plus massif aux outils digitaux notamment dans les domaines de l'expérience client et de l'expérience collaborateur. Bien qu'antérieur à l'épidémie, ce phénomène a été accéléré par celle-ci. Un large panel de solutions développées par des startups participent d'ailleurs efficacement à ces transformations.
Pour autant, ce nouveau paradigme crée de nouvelles opportunités pour les cybercriminels. Force est de constater que la cybersécurité reste encore une discipline complexe, accessible aux seuls spécialistes du sujet. Si cela n'est pas problématique pour les grands groupes qui ont la capacité à recruter ces spécialistes, la situation est très différente pour les PME-ETI qui elles n'ont bien souvent pas la capacité d'internaliser cette compétence.

Ce guide fait suite à une conférence organisée en mars 2021. Il a pour objectif d'apporter les principales clés de compréhension de la problématique "cybersécurité" aux dirigeants de PME / ETI. A titre d'illustration, Il présente le principe de fonctionnement des solutions portées par nos intervenants. Pour autant ces outils ne sont pas uniques sur le marché et nous avons également cité leurs alternatives.

Bonne lecture !

SOMMAIRE

INTRODUCTION

L'accélération fulgurante de la transformation numérique coïncide avec la croissance des cybermenaces. Selon la société McAfee, la cybercriminalité (détournements de données, demandes de rançons ...) coûte 600 milliards de dollars par an à travers le monde, soit 0,8 % du produit intérieur brut (PIB) mondial.

« *La cybercriminalité n'est qu'une évolution de la criminalité traditionnelle et a un impact direct sur la croissance économique, l'emploi, l'innovation et l'investissement. Les entreprises doivent comprendre que, dans le monde actuel, le cyber-risque est un risque commercial.* » affirme Raj Samani, scientifique en chef de McAfee
(https://www.lesechos.fr/2018/02/la-cybercriminalite-coute-600-milliards-de-dollars-par-an-984995)

L'inventaire des cyber attaques, réalisé par MagIT et Valéry Rieß-Marchive, montre une évolution de +17% en décembre 2021 par rapport à la moyenne de 2021. Ce calcul montre qu'à ce rythme les attaques vont être multipliées, à minima, par 1.000 d'ici 10 ans.
Ces menaces évoluées exigent des solutions de sécurité intelligentes.
https://www.lemagit.fr/actualites/252512782/Ransomware-les-chiffres-dun-phenomene-explosif

Pour que ces solutions soient véritablement performantes lors de leur déploiement, il est essentiel de trouver le juste équilibre entre l'automatisation et la place à accorder à l'humain.

Le 22 avril 2021, le Club Essor Innovation de Paris&Co a organisé son premier Séminaire Flash sur la cybersécurité avec la collaboration de nombreux experts, parmi les meilleurs en France, à ce sujet.

L'objectif principal de ce séminaire était de permettre aux PME/ETI de se familiariser avec tout ce qu'implique la Cybersécurité en entreprise. Une sensibilisation sur le sujet (surface d'attaque, diagnostic des menaces, mode opératoire des pirates) et la présentation de solutions (certificats, prévention, cyberdéfense, renforcement) ont été les principaux axes de ce séminaire.

En parallèle, le Club Essor Innovation a structuré des rendez-vous de sensibilisation et diagnostic en partenariat avec la société Cyber4U.

Ce guide vous présente une synthèse des bonnes pratiques, solutions et outils adaptés aux PME et ETI.

Ce contenu est issu du Séminaire Flash sur la cybersécurité pour les PME et ETI du Club Essor Innovation. Nous adressons tous nos remerciements aux intervenants :

- Sébastien Dupont, Directeur Cyber4U, Expert Cybersécurité
- Mauro Israël, CISO Advisor - RSSI de transition, Expert Cybersécurité
- Jean-Luc Louazon, Expert Cybersécurité
- Alain Bouillé - Délégué Général, CESIN
- Didier Savalle - Responsable Régional, Club 27001
- Yassir Kazar, CEO & Co-fondateur, Yogosha
- Jean-Nicolas Piotrowski, Président, Itrust
- Maxime Alay-Eddine, CEO & Co-fondateur, Cyberwatch
- Ingrid Söllner, Chief Marketing Officer, Tehtris

- 1 -

Etat des lieux de la cybersécurité en France

« L'ENISA (European Union Agency for Cybersecurity) Threat Landscape fournit une vue d'ensemble des menaces, ainsi que des tendances actuelles et émergentes. Il est basé sur des données publiquement disponibles et fournit un point de vue indépendant sur les menaces observées, les agents de menaces et les tendances des menaces. Des centaines de rapports provenant de l'industrie de la sécurité, des réseaux d'excellence, des organismes de normalisation et d'autres instituts indépendants ont été analysés.

Le rapport **ENISA Threat Landscape 2020** fournit une analyse complète des 15 principales cybermenaces rencontrées entre janvier 2019 et avril 2020. »

https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

www.enisa.europa.eu
For more information : https://www.enisa.europa.eu/topics/etl

1

MALWARE

Le logiciel malveillant (malware) est une cyberattaque couramment utilisée. Dans les familles de logiciels malveillants figurent des cryptomineurs, des virus, des rançongiciels (ransomware), des vers et des espiogiciels (spyware). Ils ont pour objectifs communs de voler des informations ou d'usurper des identités, de faire de l'espionnage et de provoquer l'interruption des services.

2

WEB-BASED ATTACKS

Les attaques sur le web constituent une méthode par laquelle les auteurs de menace peuvent tromper leurs victimes en utilisant les systèmes et services du web comme vecteur d'attaque. Elles couvrent une vaste gamme d'attaques soit en dirigeant l'utilisateur ou la victime vers le site web souhaité activant le téléchargement d'un malware, soit en injectant du code malveillant dans un site web légitime mais compromis dans le but de voler des informations, de gagner de l'argent, voire d'extorquer des fonds par le biais d'un rançongiciel (ransomware).

3

PHISHING

L'hameçonnage (phishing) est une technique frauduleuse qui consiste à voler des données d'utilisateur comme des identifiants de connexion, des informations de carte bancaire, voire de l'argent, en utilisant des méthodes d'ingénierie sociale (social engineering). Ce type d'attaque est généralement lancé par messages électroniques, semblant provenir d'une source fiable, dont le but est de persuader l'utilisateur d'ouvrir une pièce jointe malveillante ou de cliquer sur une URL frauduleuse. Une forme ciblée d'hameçonnage appelée spearphishing s'appuie sur des recherches préalables concernant les victimes afin que l'arnaque semble plus authentique ; c'est pourquoi ce type d'attaque est l'une des plus efficaces sur les réseaux d'entreprises.

4

WEB APPLICATION ATTACKS

Les applications et technologies web sont devenues un élément central de l'internet en adoptant différents usages et fonctionnalités. L'augmentation de la complexité des applications web et la généralisation de leurs services créent des difficultés pour les protéger contre des menaces aux motivations diverses, allant du préjudice financier à l'atteinte à la réputation, en passant par le vol d'informations critiques ou personnelles.

5

SPAM

Le premier pourriel (spam) a été envoyé en 1978 par un responsable marketing à 393 personnes via ARPANET. Il s'agissait d'une campagne publicitaire pour un nouveau produit de la société pour laquelle il travaillait : la Digital Equipment Corporation. Pour ces 393 premiers destinataires et malgré la nouveauté de l'idée, ce pourriel reçu s'est révélé aussi agaçant qu'il le serait de nos jours. Il est désagréable de recevoir des pourriels, mais ces envois peuvent également offrir la possibilité aux acteurs malveillants de voler des informations à caractère personnel ou d'installer un logiciel malveillant (malware).

6

DENIAL OF SERVICE

Les attaques par déni de service distribué (DDoS - Distributed Denial of Service) se produisent lorsque les utilisateurs d'un système ou d'un service ne sont pas en mesure d'accéder aux informations, services ou autres ressources concernés. Cette étape peut être franchie en épuisant le service ou en surchargeant un élément de l'infrastructure réseau. Ce type d'attaque est très utilisé pour rendre inactif un site internet. Les acteurs malveillants ont augmenté le nombre d'attaques en ciblant davantage de secteurs avec des motifs différents.

7

IDENTITY THEFT

L'usurpation d'identité ou la fraude à l'identité est l'utilisation illicite des données d'identification d'une victime par un imposteur pour se faire passer pour cette personne afin d'obtenir un avantage financier et d'autres bénéfices. Selon un rapport annuel sur la sécurité, au moins 900 cas internationaux d'usurpation d'identité ou de délits liés à l'identité ont été détectés en 2019.

8

DATA BREACH

Une violation de données est un type d'incident de cybersécurité au cours duquel des informations (ou une partie d'un système d'information) sont consultées sans l'autorisation appropriée, généralement à des fins malveillantes, donnant lieu à la possible perte ou utilisation abusive de ces informations. Elle comprend également l'«erreur humaine» qui se produit souvent lors de la configuration et du déploiement de certains services et systèmes, et qui peut entraîner une exposition involontaire de données.

9

INSIDER THREAT

Une menace interne est une action pouvant aboutir à un incident, mise en œuvre par un individu ou un groupe d'individus affiliés à une victime potentielle ou travaillant avec celle-ci. Il existe plusieurs schémas associés aux menaces provenant de l'intérieur. Un schéma de menace interne bien connu se produit lorsque des personnes extérieures collaborent avec des acteurs internes pour obtenir un accès non autorisé à des actifs. Les initiés peuvent causer des dommages involontaires par imprudence ou par manque de connaissances. Dans la mesure où ces initiés jouissent généralement de confiance et de privilèges, en plus de la connaissance des politiques, processus et procédures de l'organisation, il est souvent bien difficile de faire la distinction entre accès légitime, accès malveillant et accès erroné aux applications, données et systèmes.

10

BOTNETS

Un réseau de machines zombies (botnet) est un réseau d'appareils connectés qui sont infectés par un logiciel malveillant de type robot (bot). Ces appareils sont généralement utilisés par des acteurs malveillants pour mener des attaques par déni de service distribué (DDoS - Distributed Denial of Service). Fonctionnant en mode poste-à-poste (P2P - Peer-toPeer) ou depuis un centre de commande et de contrôle (C&C), les réseaux de machines zombies sont contrôlés à distance par un acteur malveillant pour garantir une synchronisation du fonctionnement afin d'obtenir un certain résultat

11

PHYSICAL MANIPULATION, DAMAGE, THEFT AND LOSS

Les risques liés à la manipulation physique, aux dommages, au vol et aux pertes ont radicalement changé ces dernières années. L'intégrité des appareils est essentielle pour la mobilité de la technologie et pour la plupart des déploiements de l'internet des objets (IoT - Internet of Things). L'IoT est en mesure de renforcer la sécurité physique grâce à des solutions plus avancées et plus complexes.

12

INFORMATION LEAKAGE

Une violation de données survient lorsque les données, dont une organisation est responsable, subissent un incident de sécurité qui entraîne une violation de la confidentialité, de la disponibilité ou de l'intégrité. Une violation de données entraîne souvent une fuite d'informations, qui constitue l'une des principales cybermenaces, couvrant un large éventail d'informations compromises allant des données à caractère personnel aux données financières stockées dans les infrastructures informatiques, en passant par les renseignements personnels sur la santé conservés dans les référentiels de prestataires de soins.

13

RANSOMWARE

Le rançongiciel (ransomware) est désormais une arme populaire entre les mains d'acteurs malveillants qui tentent quotidiennement de nuire aux gouvernements, aux entreprises et aux particuliers. Dans ce cas, la victime du rançongiciel est susceptible de subir des pertes économiques, soit en payant la rançon demandée, soit en payant les frais de recouvrement de la perte si celle-ci ne respecte pas les exigences de l'attaquant.

14

CYBER ESPIONNAGE

Considéré à la fois comme une menace et un mobile dans la stratégie de cybersécurité, le cyber espionnage se définit comme l'utilisation des réseaux informatiques pour obtenir l'accès illicite à des informations confidentielles, généralement détenues par un gouvernement ou une autre organisation.

15

CRYPTOHACKING

Le cryptominage (également connu sous le nom de cryptojacking) est l'utilisation non autorisée des ressources d'un appareil pour miner des cryptomonnaies. Les cibles sont généralement des appareils connectés, tels que des ordinateurs et des téléphones portables. Cependant, les cybercriminels visent désormais de plus en plus les infrastructures en nuage.

UNE VULNÉRABILITÉ DES ENTREPRISES AUX CYBERATTAQUES TOUJOURS AVÉRÉE

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) a lancé en 2015, en partenariat avec *Opinion Way*, une grande enquête annuelle pour connaître la perception de la cybersécurité des grandes entreprises. Le CESIN consulte chaque année ses adhérents sur cette base et publie en janvier les résultats de cette enquête sur la cybercriminalité en France. Les extraits ci-dessous concernent l'édition de janvier 2021.

Cette étude a été réalisée sur 230 membres dont 36% d'ETI et 55% de grandes entreprises. Les principaux secteurs d'activité représentés étaient notamment : Services (43%), Industrie/BTP (22%), Commerce (16%) et Services Publics (16%).

Le premier enseignement est que la majorité des entreprises (6 sur 10) ont été victimes d'au moins une cyberattaque. Celles-ci ont été plus nombreuses qu'en 2019 et ont souvent impacté leur activité.

La généralisation du télétravail, qui a généré de nouvelles failles, contribue à expliquer ce constat. Dans le détail, 2020 a été marquée par une menace croissante des **ransomwares** : lors de ce type d'attaque, les pirates exigent le paiement d'une rançon à leur victime pour la récupération de leurs données. 1 entreprise sur 5 déclare avoir été victime d'une attaque de ce type.

Le phishing est le principal vecteur d'attaque utilisé. Le vol de données et le déni de service sont les conséquences directes de ces attaques. De plus, le Shadow IT (l'utilisation par les collaborateurs d'outils et matériels non validés par leur DSI) est une cause très fréquente des incidents de sécurité rencontrés par les entreprises.

En termes de protection, la majorité des entreprises considère que les solutions de protection du marché sont adaptées mais elles ne se sentent pas bien préparées. La part du budget IT consacrée à la sécurité reste stable en 2020. En revanche, 2 entreprises sur 5 prévoient d'augmenter leur budgets cybersécurité pour 2021.

En moyenne, une dizaine de solutions sont mises en place en moyenne par les entreprises interrogées. Le recours au télétravail contribue d'ailleurs à l'utilisation massive du VPN et de l'authentification multi facteurs.

Le constat est que le Cloud, aujourd'hui largement plébiscité par les entreprises, est toujours un environnement à risques en raison de la non-maîtrise et des difficultés des contrôles liées à son utilisation. Sa sécurisation nécessite des outils spécifiques, autres que ceux fournis par les prestataires Cloud. Il est d'ailleurs important de rappeler que **pour faire face à ces menaces, la sensibilisation des salariés est le premier dispositif à renforcer.**

A ce titre, soulignons que les risques sont parfois liés à l'usage de logiciels web anodins par certains collaborateurs : par exemple l'outil *Nitro PDF*, qui permet de convertir les fichiers en format PDF, est très utilisé en entreprise. Or cet outil a été piraté et 70 millions d'emails et de mots de passe chiffrés ont été vendus sur le dark web. Les utilisateurs ayant tendance à utiliser le même mot de passe pour différents services, le danger est bien réel (si vous souhaitez savoir si votre adresse électronique ou votre numéro de téléphone ont déjà été vendus sur le dark web, vous pouvez vous rendre sur le site « *have i been pwned* »).

En synthèse, les entreprises sont inquiètes mais clairvoyantes sur les enjeux de demain. Elles prennent de plus en plus conscience de l'importance de la cybersécurité dans la stratégie, ce qui explique que plus de la moitié d'entre elles comptent augmenter les budgets et les effectifs liés à la cybersécurité. Plus de 8 sur 10 souhaitent acquérir de nouvelles solutions techniques, dont des solutions innovantes pour se prémunir des cyber risques. Enfin, elles ont conscience de l'importance du facteur humain dans leur vulnérabilité.

Vous trouverez ci-dessous le lien pour consulter la 7eme édition du Baromètre annuel du CESIN:

https://www.cesin.fr/actu-7eme-edition-du-barometre-annuel-du-cesin-enquete-exclusive-sur-la-cybersecurite-des-entreprises-francaises.html

- 2 -

La chaîne d'attaque et les principaux modes opératoires des pirates

LE MONDE DIGITAL : UN SEUL MONDE GLOBAL - INTERCONNECTÉ - SANS FRONTIÈRES

Suite aux évolutions technologiques, le monde devient un monde digital. Contrairement au monde physique, celui-ci est un monde global. Toutes les machines de tous les pays de la planète sont interconnectées. Pour évaluer les risques, il faut être conscient des faits : il faut moins d'une seconde pour pirater un ordinateur. Un ordinateur au Chili nécessite moins d'une seconde pour attaquer votre ordinateur en France. Les pirates visent donc leurs attaques sur des lieux où ils ne sont pas situés. Ce qui rend cette cyberguerre extrêmement compliquée.

LE CONFINEMENT, LES NOUVEAUX MODES DE TRAVAIL ISSUS DE LA CRISE DU COVID-19 MODIFIENT DURABLEMENT NOTRE ÉCONOMIE ET NOTRE ORGANISATION SOCIALE

Le constat le plus évident est que les moyens informatiques que nous avons déployés au cours du télétravail créent un changement d'usage. Il faut donc une adaptation des entreprises en prenant conscience que le télétravail s'installe de manière durable dans notre économie.
La chaîne d'attaque (Cyber Kill Chain) représente les différentes étapes du mode opératoire exploité par les cybercriminels. Nous pouvons voir ci-dessous la feuille de route allant du premier contact jusqu'aux objectifs finaux :

1. **Reconnaissance :** Identification de la cible, évaluation de son potentiel économique, identification de ses vulnérabilités

2. **Armement :** L'attaquant crée le vecteur de son attaque (Virus, Cheval de troie, etc)

3. **Livraison :** le vecteur est transmis à sa cible, le plus souvent par une opération de phishing, ou via une clé USB "oubliée" etc.

4. **Installation :** le vecteur installe un point d'accès au système d'information de l'entreprise

5. **Commande et Contrôle :** intrusion et prise de contrôle progressif du système d'information de l'entreprise

6. **Exploitation :** réalisation de l'objectif (vol des données, blocage du système, déni de service, etc..)

Les cyberattaques entraînent des perturbations de l'activité, des ransomwares (demande de rançons), des vols de données personnelles et professionnelles, des fraudes financières, etc.
Si vous souhaitez obtenir des précisions sur la chaîne d'attaque, vous trouverez tous les détails techniques en consultant le rapport rédigé par Mauro Israël : https://mauro-israel.over-blog.com/

FOCUS SUR LE RANSOMWARE

Les cyberattaques par ransomware se produisent quotidiennement mais les entreprises visées communiquent très peu sur ce sujet.

Points importants concernant les ransomwares :

- Les entreprises ciblées sont bloquées dans leur activité par un ransomware qui chiffre tous les fichiers.

- Une rançon (en cryptomonnaie par exemple) est demandée contre le code de déchiffrement.

- Cette rançon est proportionnelle à la taille et l'activité de l'entreprise : de quelques centaines d'euros à plusieurs millions…

MODE OPERATOIRE LE PLUS FREQUENT

PHASE 1 :

1. Reconnaissance de la cible (visibilité de votre entreprise sur internet), analyse de surface d'attaque, vulnérabilités et points d'entrées possibles existants dans votre SI, exposition à l'internet augmentée par le télétravail (dans l'extérieur de votre périmètre) .

2. Envoi d'un email de phishing (d'un fournisseur, d'une entité gouvernementale, etc).

3. Compromis initial à la suite du clic (tels que les troyens laissant le cheval d'Ulysse rentrer au sein de leur périmètre). Le constat à ce stade est que, même bien informés et très préparés, il y aura toujours, dans une organisation de plus de 100 personnes, quelques collaborateurs qui cliqueront sur le lien malveillant.

PHASE 2 :

1. Prise de contrôle à distance (pendant quelques semaines de manière silencieuse).

2. Affichage d'un message de demande de rançon sur tout le réseau, et tous les écrans qui ont été piratés (avec une diffusion d'échantillons de données volées).

3. Maintien dans le système, dysfonctionnements et demandes de rançon à répétition (certaines entreprises paient la rançon initiale et se retrouvent de nouveau paralysées, des semaines après, par une nouvelle demande de rançon).

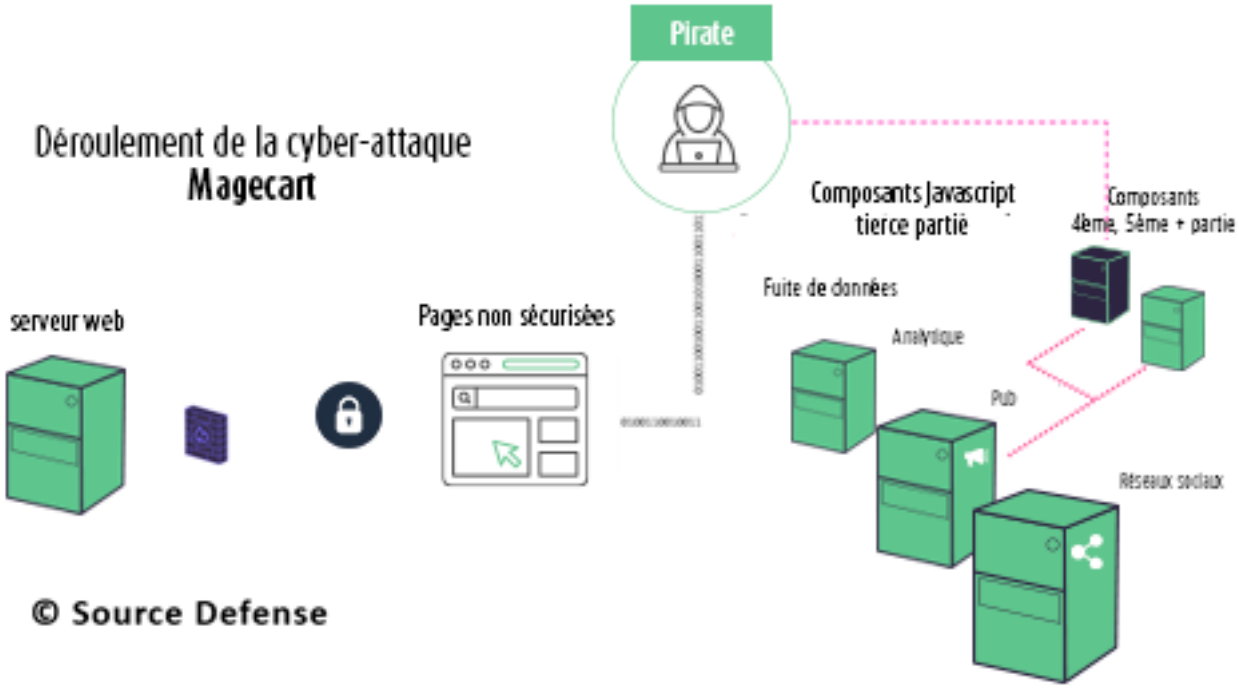
FOCUS SUR LE MAGECART : compromission des données personnelles & bancaires

Ce type d'attaque concerne tous les sites où le client saisit sa carte de crédit pour payer, donc les e-commerces.

MODE OPERATOIRE LE PLUS FREQUENT

Sur un serveur web, il existe des composants développés par des tiers (faisant eux même appel à des composants, etc) destinés à différents usages : publicité, réseaux sociaux, analytiques. Le pirate n'attaque pas directement le site web mais il cible ces composants de rang 4 ou 5. Par exemple, Facebook peut avoir 30, 40 ou 50 sous-traitants pour analyser le micro-comportement de chaque utilisateur.

Une fois le paiement effectué, rien de particulier ne se produit sur le site web ou pour l'utilisateur qui reçoit bien le produit commandé. Mais le pirate a récupéré les données bancaires de l'utilisateur et peut maintenant créer de fausses cartes avec le CVV.



- 3 -

Les moyens de lutte contre les cyberattaques

Pour contrer efficacement les cyberattaques il faut changer de paradigme :
Tout ce que nous faisions avant (antivirus, firewall...) est malheureusement obsolète aujourd'hui. La preuve étant que, malgré ces dispositifs en place, les entreprises se font toujours pirater. Le nouveau paradigme que nous devons adopter est donc celui du « *zero trust* ». Signifiant que nous ne faisons plus confiance à rien.

TOUT DOIT ÊTRE CONTRÔLÉ :

- Chaque utilisateur doit être identifié
- Chaque accès doit être validé
- Chaque composant doit être vérifié

QUATRE PRINCIPES POUR RÉDUIRE AU MAXIMUM UNE SURFACE D'ATTAQUE :

1. **Zéro surface d'attaque :**
Cartographier tout ce qui est exposé à internet et éliminer les failles de sécurité

2. **Zéro composant unique** (SPOF *single point of failure*) :
Prévoir une architecture redondante

3. **Zéro accès distant** (VPN *virtual private network* / RDP *remote desktop protocol*) :
Privilégier les accès distants au travers d'un serveur proxy permettant de filtrer le web (chaque accès distant étant potentiellement un cheval de Troie pour rentrer dans l'entreprise)

4. **Zéro accréditation « ouvre tout » :**
Privilégier des connexions différenciées aux applications web plutôt qu'une connexion unique à un « système-réseau ». Le SSO *(single sign-on)* devient un *e-coffre* des mots de passe.

2 DIMENSIONS DOIVENT ÊTRE DÉVELOPPÉES :

- La mise en œuvre d'une stratégie organisationnelle et humaine de cybersécurité
- La mise en œuvre de solutions techniques adaptées à votre entreprise

- 3.1 -

La mise en place d'une stratégie organisationnelle et humaine de cybersécurité

Cyber4U, 1er centre de cybersécurité dédié aux ETI et aux collectivités locales, partage son retour d'expérience établi au contact des organisations privées et publiques.

La mise en place de mesures outillées est urgente pour faire face aux menaces en cybersécurité. En complément, une organisation de la cybersécurité doit être implémentée afin d'apporter des garanties d'efficacité et de protection dans le temps.

Il n'existe pas de démarche unique pour une PME et une ETI. Les bonnes pratiques inspirées par les efforts réalisés par les « grands » doivent être adaptées.

Pour se limiter à 8 priorités :

1. Faire auditer le dispositif de sauvegarde / restauration des données
Elles sont trop souvent l'ultime « bouée de secours » pour certaines PME et ETI. « N*ous n'avons rien à craindre car nous avons des sauvegardes* ». C'est oublier que les dispositifs de sauvegarde / restauration sont une fois sur cinq ciblée par les attaquants (*https://www.riskinsight-wavestone.com/2021/11/cyber-attaques-quels-risques-sur-les-sauvegardes-et-comment-sen-proteger/#:~:text=Les%20attaquants%20ont%20bien%20compris,jusqu'%C3%A0%20%C3%AAtre%20rendus%20inutilisables)* qui suivent généralement la règle 321 (3 copies dont 2 sur 2 types de support de stockage + 1 copie dans le Cloud). Il convient donc de faire auditer régulièrement le niveau de robustesse du dispositif de sauvegarde vis-à-vis des attaques par rançongiciel.

2. Définir, tester et améliorer votre plan de crise cyber
Le délai de reprise des activités essentielles est d'environ 1 mois et de 5 mois pour le reste des activités pour un montant compris entre 300.000 et 1 M€. Il correspond parfois au chiffre d'affaires réalisé sur la période auquel il faut ajouter les frais des « pompiers cyber » pour « investiguer », « sortir les hackeurs » et « reconstruire ».

Malgré les mesures prises, il convient de se préparer à la crise. Un exercice de crise cyber permet notamment de se rendre compte des échelles de temps et des moyens nécessaire pour reconstruire une « bulle de confiance » saine afin de redémarrer les activités essentielles.

3. Instaurer la double authentification et acculturer les utilisateurs
Le vol de seulement quelques comptes utilisateurs au sein d'une entreprise est suffisant mener une opération de rançongiciels. La double authentification est donc recommandée pour les utilisateurs et « très fortement conseillée » pour tous les comptes à privilèges.
Les utilisateurs doivent être sensibilisés aux dangers et aux bonnes pratiques. Il est recommandé aux PME et ETI d'utiliser les sources publiques ou de déléguer cette sensibilisation. Il est pertinent d'éviter de construire de zéro un programme, ce qui est chronophage au regard des autres actions Cyber à mener. Il est également pertinent d'assurer la cohérence du programme de sensibilisation avec la charte d'usage des ressources informatiques, qui est rattachée au règlement intérieur.

4. Adopter les dispositifs modernes de la cybersécurité en commençant par l'EDR
Les antivirus ne protègent que de 40% des attaques. Les dispositifs modernes à mettre urgemment en place sont l'EDR, le SIEM et le SOC qui va superviser les alertes et permettre une amélioration continue. D'autres briques sont pertinentes dans de nombreux cas : le « Bastion » pour protéger les comptes à privilèges et le « WAF » pour protéger des attaques applicatives. Durcir les composants sensibles, comme l'Active Directory, qui intervient dans 100% des attaques, est également un incontournable.

5. Chasser les vulnérabilités en gérant les correctifs de sécurité des équipements IT
Avec près de 20.000 vulnérabilités découvertes par an, toutes technologies confondues, il est essentiel d'attribuer cette mission au sein de son organisation, d'allouer les moyens nécessaires et de contrôler. Dans près de 50% des attaques réussies, l'exploitation d'une vulnérabilité connue est en cause. Le défi à relever nécessite un réel effort collectif et les outils de détection de vulnérabilités apportent une aide bienvenue.

6. Prendre en compte la cyber dans les nouveaux projets IT
Une fois que les fonctions transverses de la sécurité sont mises en place, il est pertinent d'embarquer les nouveaux projets dans la démarche sécurité. Le « Security By Design » peut s'appuyer sur des référentiels de bonnes pratiques (règles de gestion des authentifiants de l'ANSSI, fiches CNIL, TOP10 OWASP,…). Cette préoccupation répond à l'article 32 du RGPD. En complément, des clauses de sécurité type sont à établir pour les contrats avec les sous-traitants.

7. Disposer d'une Politique de Sécurité pour instaurer la démarche dans la durée
La Politique Générale de Sécurité des Systèmes d'Information (PGSSI) va permettre de définir les grandes orientations retenues pour défendre la PME, l'ETI, la collectivité locale ou l'hôpital vis-à-vis des risques cyber. Il s'agit d'aligner les acteurs de l'entreprise dans cette direction : Direction, Management intermédiaire, Equipes projets, Utilisateurs. Les principaux processus cyber sont identifiés, tout comme les responsabilités associées : gestion des correctifs, évaluation de l'efficacité des mesures, arbitrage des risques.

8. Animer la sécurité : piloter les chantiers, préparer le comité sécurité, rédiger les procédures, lancer les audits
Se défendre en cyber nécessite de passer à l'action. « *Il n'y a pas de sécurité, il n'y a que des mesures de sécurité* ». Cela nécessite des moyens humains pour animer la cybersécurité. Faire appel à un « RSSI externe à temps partagé » est une piste intéressante pour les PME et les ETI. La documentation cyber doit permettre d'agir efficacement (ex : que faire en cas de mail suspect ?) mais également de rendre compte de la cybersécurité auprès de la Direction pour instaurer un véritable pilotage.
Les audits sont un moyen simple et peu coûteux pour « éclairer » un périmètre à mettre sous contrôle. Ils sont sous-utilisés par les PME et les ETI.

- 3.2 -

La mise en œuvre de solutions techniques adaptées à votre entreprise

NOTICE EXPLICATIVE SUR LES SOLUTIONS PRÉSENTÉES :

Ce guide fait suite à une conférence organisée en mars 2021. Nous avions invité un certain nombre de représentants de sociétés proposant des outils adaptés aux PME/ ETI. Le choix a été réalisé en fonction de la proximité de ces acteurs, recommandés par nos experts, avec notre écosystème Paris&Co. Nous avons donc détaillé leurs solutions dans ce guide, dont la vocation première est d'illustrer le mode de fonctionnement de ce type d'outils.

Il n'y a aucun sponsoring financier de ces intervenants pour la réalisation de ce guide et l'objet n'est pas de recommander ou promouvoir leurs solutions en particulier. Nous proposons, à l'issue de chaque présentation, 1 à 4 solutions toutes aussi pertinentes et qualitatives. Il appartient à chacune de faire sa propre sélection en fonction de ses besoins.

Vous pourrez retrouver la liste des professionnels recommandés à l'adresse suivante :
https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/professionnels-en-securite-informatique

DIAGNOSTIC DE LA SURFACE D'ATTAQUE

La première étape pour structurer une stratégie de cybersécurité est de faire un diagnostic de la surface d'attaque de votre entreprise. Ces diagnostics sont proposés par une grande variété de prestataires : ces missions peuvent être réalisées par des consultants certifiés, des experts, des startups, etc. Vous devrez choisir l'offre la plus adaptée à votre contexte, à vos besoins et à votre budget. Ce diagnostic met en lumière vos faiblesses et vos failles spécifiques qui doivent être corrigées.

Une fois le diagnostic effectué et les correctifs spécifiques définis, un plan d'action devra être lancé afin de renforcer le niveau de sécurité de votre système d'information. A ce moment-là, vous devrez évoluer du diagnostic à la protection grâce aux outils présentés ci-après. *

Mauro Israël, expert en cybersécurité, propose : « *Les certificats, les bases SQL, les transferts de fichiers... sont les éléments que nous allons diagnostiquer. Il faut garder à l'esprit que tous ces éléments sont visibles par les pirates. Lorsqu'ils sont en phase de reconnaissance, ils vont scanner vos vulnérabilités pour définir leur stratégie d'attaque. Nous aurons un plan d'action simple, corrigeant toutes les failles de sécurité où vous pourriez être attaqué. Par ailleurs, nous allons aussi recourir à des normes nous donnant une certaine conformité, telles que l'ISO 27001, ou d'autres normes internationales : la Payment Card Industry DSS Version 3.1 et la conformité au RGPD (obligatoire pour toutes les entreprises).* »

Plusieurs outils permettent de réaliser un diagnostic de surface d'attaque : Security Scorecard, Cyrating, Almond Consulting, etc...

A titre d'exemple, le processus pour réaliser gratuitement un diagnostic avec Security Scorecard est le suivant :

- *Vous rendre sur le site de Security Scorecard : https://securityscorecard.com/fr*
- *Créer un compte sur le lien suivant : https://securityscorecard.com/free-account*
- *Il est nécessaire que l'email que l'on indique corresponde au domaine, par exemple prénom.nom@votre_nom_de_domaine.com pour le domaine votre_nom-de_domaine.com*

La Cartographie des outils disponibles
Si vous êtes une PME il vous sera difficile d'appliquer toutes les mesures de cybersécurité simultanément, vous devrez donc vous concentrer sur les vulnérabilités existantes qui pourraient vous atteindre le plus. Une fois que vous avez réduit votre surface d'attaque, il faut se concentrer sur quatre éléments principaux :

1. SOC (Alerte & Gestion des incidents)
2. Vulnérabilités et Patches
3. EDR : Endpoint detection and response
4. Bug Bounty

Avant d'entrer dans le détail de ces outils, il est important de développer la notion de Read Team et Blue Team souvent utilisée par les professionnels. En effet, dans le monde de la cybersécurité, les experts distinguent **2 types de prestations** :

- **Blue Team (ISO 27001) :** sécurité défensive, protection infrastructure, réponse à incidents, scan de vulnérabilité, forensique.

- **Red Team:** sécurité offensive, *ethical hacking*, test intrusion interne-externe, boites noire-grise-blanche, social engineering (nous retrouverons ces éléments à la fin du document avec les solutions proposées par les startups).

1) SOC - SECURITY OPERATION CENTER

Nous pouvons considérer le SOC comme étant le service d'urgence du cyber-hôpital.

Si un hôpital a des médecins pour réaliser les soins, il a également besoin d'une analyse des malades en amont pour déterminer la gravité de la pathologie du patient.

Dans le contexte du SOC, il y a également un processus de sélection pour trier les cas (les moins critiques, les faux positifs…) et détecter les signaux de vulnérabilité, car une petite alerte qui est passée inaperçue peut cacher une forte attaque potentielle.
Une fois que l'équipe d'analystes a trié les attaques, elle identifie celles qui doivent être traitées ou pas. L'entreprise reçoit des millions d'événements par jour, ce qui fait des analyses SOC un travail extrêmement complexe.

Après avoir effectué une investigation approfondie sur le deep web, les analystes du SOC vont trouver des solutions. Ils contactent l'appareil ou l'utilisateur qui a été compromis, et mettent en place un plan d'action qui leur permettra de bloquer l'attaque.

EXEMPLE DU MODE OPÉRATOIRE DU SOC :
Le SOC présente en temps réel au sein d'un tableau de bord, les millions de moments de vie du système d'informations de l'entreprise qui créent des alertes (patterns of life). Le SOC intègre une intelligence artificielle qui permet de faire un tri parmi ces alertes.

Par exemple il détecte une connexion anormale à un serveur Microsoft en Hollande qui n'a jamais été utilisée auparavant. Et que l'utilisateur en question est en train d'envoyer une source d'information très volumineuse vers une connexion externe.

Les analystes vont examiner les données qui ont été envoyées ainsi que leur destination. Ils se rendent alors compte que les informations ont été transférées vers six serveurs différents par la machine en question. C'est une information suffisamment suspicieuse pour ouvrir une investigation, afin de déterminer s'il s'agit d'une cyberattaque. Les analystes vont contacter la personne qui opère cette machine et voir pourquoi cet utilisateur a transféré un tel volume de données vers un serveur externe.

Suite aux échanges avec l'utilisateur en question, les analystes ont réalisé que celui-ci sauvegardait ses documents sur un « onedrive » Microsoft hébergé en Hollande, seul moyen pour lui d'accéder à ses documents et de travailler à distance. Cette situation était donc, comme la plupart des alertes traitées, un faux positif. Elle est néanmoins susceptible de créer une vulnérabilité.

L'IMPORTANCE DE LA SENSIBILISATION :
Dans l'exemple précédent, l'utilisateur a sorti des données hors de l'entreprise en toute bonne foi car il n'avait pas d'autres moyens accomplir ses tâches professionnelles. C'est pourquoi la sensibilisation des employés est primordiale dans le dispositif de lutte contre les cyberattaques. Nous pouvons ainsi mesurer l'importance du rôle du SOC, qui sera en veille 24/7 pour questionner tout mouvement suspect. Est-ce une fuite d'informations ? Est-ce volontaire ? Involontaire ?

Pour la sécurité d'une entreprise, disposer d'un service d'urgence en veille 24/7 est donc crucial. Si une attaque a lieu en dehors des heures de bureau, celle-ci sera traitée à la seconde même. Les pirates n'attaquent pas les entreprises que pendant leurs horaires d'ouvertures, ils utilisent justement les périodes estivales, week-ends, ponts, jours fériés de chaque pays.

En conclusion, la mise en place de contrôles et politiques de sécurité adaptés à chaque activité est un élément essentiel de la protection d'une entreprise. Grâce à la sensibilisation, les employés seront informés des procédures, des politiques et des meilleures pratiques. Des modules de formation, appliqués de manière pédagogique, permettent non seulement de s'assurer que le personnel connaît ces principes, mais aussi qu'il les suit et les comprend.

EXEMPLE D'OUTIL SOC ADAPTÉ AUX PME ETI : ITRUST

ITrust est un éditeur de solutions innovantes en cybersécurité. Fondée en 2007 par des passionnés de cybersécurité, l'entreprise mène des activités de services (conseil, audit, MSSP, SOC) et d'édition de logiciels de cybersécurité. ITrust propose ses produits en France et à l'étranger, via ses partenaires en marque blanche. Attachés à la souveraineté des données, les solutions sont développées en France, non soumises aux Patriot Act et Cloud Act et leur SOC Reveelium est le seul à ce jour à être labélisé U.A.F par le Ministère des Armées. ITrust protège les PME, ETI, Grands Groupes ainsi que les entreprises sensibles (OIV, OSE) contre les cybermalveillances, attaques de phishing, cryptolockers, ransomwares aussi bien en préventif qu'en détection. Le SOC d'ITrust s'appuie en effet sur des algorithmes de Machine Learning développés en interne, un moteur de Threat Intelligence et l'expertise d'analystes expérimentés pour détecter les menaces, connues ou inconnues, auxquelles fait face une entreprise.

https://www.itrust.fr

AUTRES SOLUTIONS :

- Advens : https://www.advens.fr/
- Cyber4u (SOC/SIEM/EDR) : https://cyber4u.fr/
- Intrinsec : https://www.intrinsec.com/
- Orange Cyberdéfense (Microsoc) : https://orangecyberdefense.com/fr/services/management-support/microsoc/
- Tracing : https://i-tracing.com/

2) VULNÉRABILITÉ ET PATCHES

La gestion des correctifs consiste à maintenir les logiciels des ordinateurs, équipements de réseau et serveurs à jour afin qu'ils soient capables de résister à des cyberattaques de bas niveau. Tout logiciel est régulièrement testé par des chercheurs en sécurité informatique, et peut donc faire l'objet de vulnérabilités techniques. Une fois découvertes et rendues publiques, celles-ci sont immédiatement exploitées par les cybercriminels.

Afin d'identifier les correctifs qui doivent être traités, vous devrez effectuer un diagnostic de votre surface d'attaque (qui a été mentionnée précédemment dans le document).

Une fois ce diagnostic effectué, l'outil vous présentera le panorama des correctifs de sécurité et des normes qui n'ont pas encore été mis en place.

Il est à noter que le télétravail généralisé rend les systèmes dont les composants ne sont pas mis à jour, plus vulnérables. En effet, les gestionnaires de réseau, également en télétravail, utilisent des connexions externes pour accéder aux serveurs de l'entreprise. Les pirates exploitent alors le fait que le système d'administration à distance (accès VPN, SSH, Bureau à distance…) ne contient pas tous les correctifs de sécurité nécessaires pour exploiter une vulnérabilité connue et se connecter en tant qu'administrateurs.

EXEMPLE D'OUTIL DE SCAN DE VULNÉRABILITÉS AVEC DÉPLOIEMENT DE CORRECTIFS ADAPTÉ AUX PME ETI : CYBERWATCH

Cyberwatch Vulnerability Manager est une solution de gestion des vulnérabilités, avec cartographie du système d'information, détection des vulnérabilités, priorisation basée sur le risque et sur les contraintes métiers, aide à la décision, et module de correction.

Cyberwatch Compliance Manager est une solution de contrôle des conformités, avec analyse du niveau de durcissement et personnalisation complète possible des règles et des référentiels testés.

La suite complète Cyberwatch, déployée dans votre réseau (On-Premise), avec ou sans-agent, vous permet ainsi de gérer les vulnérabilités de vos actifs afin de lutter contre les menaces externes, et de contrôler la conformité de votre système d'information afin d'atteindre vos objectifs de durcissement.

https://cyberwatch.fr

AUTRES SOLUTIONS :

- Qualys : https://www.qualys.com/
- Tenable : https://fr.tenable.com/

3) EDR : ENDPOINT DETECTION AND RESPONSE

L'EDR est en quelque sorte un "super antivirus" global plus résistant au ransomware et aux attaques. Il s'agit d'une solution intégrée de sécurité qui associe la surveillance continue en temps réel et la collecte de données des "end-point" (postes de travail), avec des réponses automatisées basées sur des critères précis et des capacités d'analyse.

Il apporte une solution aux problèmes générés par le travail à distance, souvent réalisé sur des machines obsolètes, exposées à l'internet, notamment en home office. Cela concerne par exemple le navigateur ou le système d'exploitation.

Par exemple, si Windows 7 n'est pas maintenu, cela signifie qu'il n'y a plus de correctifs de sécurité disponibles, et que ces machines ne sont plus sécurisées. Il faut les arrêter, ou les upgrader vers un OS plus récent.

Ci-dessous, vous pourrez constater que **le système d'exploitation est périmé** et qu'il est donc nécessaire de mettre en place un nouveau système d'exploitation doté d'un dispositif antiviral capable de travailler sur les attaques et les comportements actuels des pirates.
En effet**, les correctifs n'existent plus pour ces systèmes obsolètes.**

	MANUFACTURER	PRODUCT	VERSION	STATUS	SOURCE IP
☐	Microsoft	Windows 7	7	end of service	194.15[redacted]
☐	Microsoft	Windows 7	7	end of service	194.15[redacted]
☐	Microsoft	Windows 7	7	end of service	91.21[redacted]
☐	Microsoft	Windows XP	XP	end of service	91.21[redacted]

EXEMPLE D'OUTIL EDR ADAPTÉ AUX PME ETI : TEHTRIS

TEHTRIS EDR embarque de nombreux moteurs de détection et de neutralisation capables d'analyser les menaces connues ou inconnues. Il neutralise les attaques en temps réel.

Il est compatible avec tous les OS, même les versions obsolètes. Il permet de défendre efficacement le parc informatique contre les cyberattaques ainsi que les comportements malveillants, avec une remédiation hyper automatisée, c'est-à-dire sans intervention humaine.

En production depuis 2013, TEHTRIS EDR est une solution souveraine, développée et hébergée en France et en Europe. Fournie en mode SaaS, elle peut être utilisée en stand-alone ou intégrée dans la TEHTRIS XDR Platform. Cette plateforme agit 24h/24 et 7j/7 pour faciliter la tâche des analystes des entreprises.

Avec 11 ans de R&D au service d'une protection et visibilité 360°, TEHTRIS propose un catalogue de solutions modulaires de cybersécurité (EDR, EPP, MTD, UES, SIEM, ZTR, NTA...) pour protéger l'ensemble des endpoints, des réseaux ou le Cloud.

Aujourd'hui, TEHTRIS est le seul éditeur européen à avoir obtenu la reconnaissance de Gartner, en étant référencé comme fournisseur représentatif dans leur Market Guide for Extended Detection & Response 2021.

https://tehtris.com/fr/.

AUTRES SOLUTIONS :

- Crowdstrike : https://www.crowdstrike.fr/
- Cybereason : https://www.cybereason.com/fr/
- HarfangLab : https://www.harfanglab.io/
- SentinelOne : https://fr.sentinelone.com/

4) BUG BOUNTY

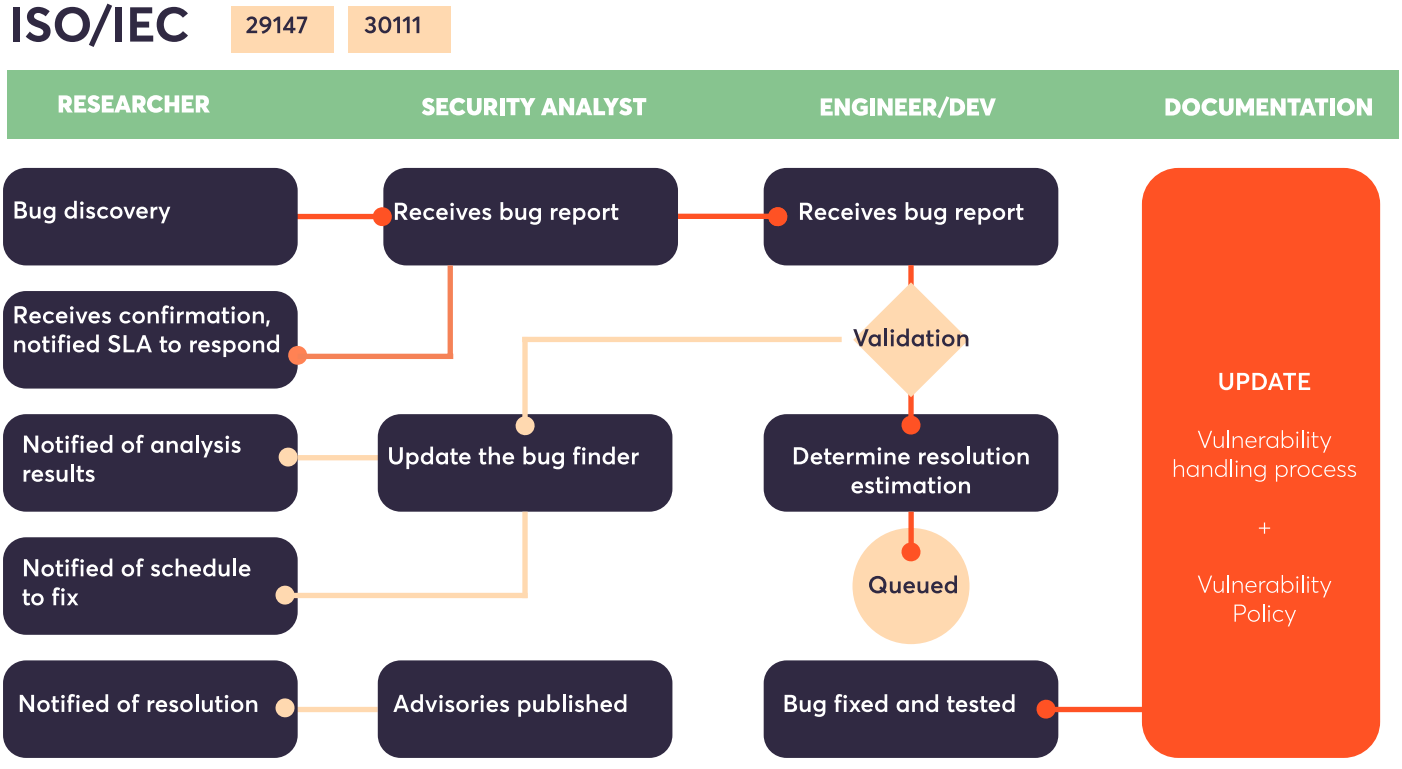
Le bug bounty ou VRP (Vulnerability Rewards Program) est une manière très innovante de vérifier les vulnérabilités sur les SI. Il s'agit d'une initiative de crowdsourcing qui consiste à récompenser des hackers éthiques pour la découverte et le signalement de software bugs. Ces programmes sont mis en place pour fournir des audits de codes internes et des tests de pénétration (pentests) dans le cadre de la stratégie de gestion des vulnérabilités et cybersécurité d'une entreprise.
La récompense dépend généralement de la taille de l'organisation, de la difficulté d'attaquer le système et de l'impact que le bug aurait pu avoir sur l'entreprise.

Ex : Google a payé 6,7 millions de dollars de récompense de bug bounty en 2020. Une somme en hausse par rapport aux 6,5 millions de dollars versés aux chercheurs en sécurité en 2019. (Catalin Cimpanu, ZDNet) https://www.zdnet.fr/actualites/cybersecurite-google-a-verse-67-millions-de-dollars-en-bug-bounty-en-2020-39917537.htm.

NORMES ET STRUCTURE DU BUG BOUNTY

« *Le bug bounty est très bien structuré, car le programme est appliqué sur différentes normes et garanties. La pratique de ce type d'attaques est importante pour matérialiser concrètement ce qui pourrait arriver à une entreprise en termes de cyberattaque. Cette opération est indispensable pour développer une stratégie en matière de cyberdéfense. Autrement, le sujet reste entièrement théorique.* » précise Yassir Kazar, CEO et co-fondateur de Yogosha.

L'idée est de consacrer un budget spécifique et payer une communauté de hackers éthiques par faille détectée. Cela signifie que chaque fois qu'une faille est détectée, et qu'elle est valide, l'entreprise la paiera. Tant que ce budget existe, les hackers pourront continuer à travailler. Cela permet à 25, 20 ou même 200 hackers de travailler sur un même système, puisque le principe du bug bounty est le suivant : le premier qui trouve la faille est celui qui est payé.



Yogosha - Confidential - 2021

Diagramme illustrant un processus de bug bounty.

EXEMPLE D'OUTIL DE BUG BOUNTY ADAPTÉ AUX PME/ETI : YOGOSHA

Yogosha est une plateforme de cybersécurité reposant sur une communauté de hackers d'élite certifiés pour la détection et la gestion des vulnérabilités d'applications les plus critiques. Programmes Bug Bounty, Pentests crowdsourcés ou CVD, le client a la possibilité de choisir sa stratégie de de sécurité et d'interagir avec les hackers.

Yogosha a ainsi créé un processus de sélection drastique pour s'assurer de la compétence et de la compliance des hackers de sa communauté. Seuls 15% passent les tests de certification techniques et pédagogiques. Chaque hacker de la communauté est connu, identifié et validé sur sa réputation et son statut fiscal.

La plateforme SaaS de Yogosha est simple à utiliser et permet de définir rapidement ses challenges de sécurité, d'analyser les rapports de vulnérabilité, la performance des campagnes et de faciliter les plans de remédiation et la correction des failles.

Yogosha

AUTRES SOLUTIONS :

- YesWeHack : https://www.yeswehack.com/fr/

La norme ISO 27001

L'ISO 27001, est une norme créée par l'ISO et IEC en 2005. Elle spécifie les exigences relatives aux Systèmes de Management de la Sécurité de l'Information (SMSI).

Les mesures de sécurité préconisées concernent toutes les entreprises, quelle que soit leur taille. Cette sécurité porte sur les humains, la technologie et les processus.

Elle encourage l'entreprise à cadencer la **Gestion de son Système d'information**, en marquant 4 étapes successives et récurrentes d'Etat des Lieux, de Planification, de Mise en Œuvre et de Vérification.

La norme ISO 27002 définit un ensemble de « bonnes pratiques » en matière de sécurité répartie en plusieurs chapitres. L'entreprise dispose alors d'un référentiel de mise en œuvre et d'une « check-list » en cas d'audit.

Le principe de la norme **ISO 27001** à l'instar d'autres normes **ISO**, est **l'Amélioration Continue**, qui part du principe que le **Système d'Information** est sans cesse **perfectible**.

La certification délivrée par un organisme accrédité suite à un audit, garantit qu'une organisation respecte bien les exigences de la norme en matière de sécurité. Cette certification est valable 3 ans et nécessite un audit de contrôle tous les ans.

Cette certification peut être nécessaire pour accéder à certains contrats. De plus, de nombreux assureurs commencent à l'intégrer dans leurs conditions commerciales et leurs grilles de tarifs.

La promotion de la norme est notamment assurée par le Club 27001, association créée en 2005 et constituée de 300 professionnels concernés par la norme.

La cybersécurité peut coûter cher, mais il coûtera plus cher de ne rien faire !

Comme nous l'indiquions en introduction, les cybermenaces risquent, à minima, d'être multipliées par 1.000 d'ici 10 ans. En tenant compte de la vitesse de l'hyper digitalisation dans la vie de tous les jours, il y a un risque réel que ce seuil soit même dépassé. Il est donc impératif de mettre en place des stratégies visant à prévenir les attaques, au lieu d'attendre d'être attaqué pour agir.

Nous avons constaté que de nombreuses actions concrètes doivent être déployées afin de créer et mettre en place un plan de cybersécurité efficace et stratégique au sein d'une entreprise. Mais la démarché doit être progressive et adaptée au contexte de la société. Nous nous sommes focalisés dans ce document sur le cas des PME ETI, avec des outils moins coûteux et une organisation moins complexe.

Le problème de l'arbitrage financier dans l'investissement cybersécurité est qu'il met en regard un coût réel face à une dépense potentielle d'un montant inconnu en cas d'attaque. Il n'existe pas véritablement de méthode d'évaluation du retour sur investissement. Le témoignage des victimes demeure malheureusement le principal outil de promotion.

Mais la cybersécurité, est aussi une question de stratégie d'investissement au plus haut niveau d'une entreprise. Si le « top management » n'inclut pas des mesures et des plans d'action de cybersécurité dans sa feuille de route stratégique, l'entreprise perdra une part de sa crédibilité. Ces mesures doivent être prises avec un point de vue d'entrepreneur car, aujourd'hui, en disposer est un sérieux avantage compétitif.

En effet, de nombreuses entreprises de référence ont réalisé que les dernières technologies, bien sécurisées, peuvent faire plus qu'améliorer le back-office. Elles peuvent également transformer le front office et permettre à une entreprise d'introduire des modèles économiques davantage centrés sur le client. Désormais, si les entreprises intègrent la cybersécurité dans la conception des produits ou des services, elles peuvent offrir une expérience client qui génère des revenus plus importants.
Les entreprises savent désormais qu'elles peuvent renforcer leur marque et fidéliser leurs clients en instaurant une « confiance digitale » avec eux. Lorsqu'une entreprise se consacre véritablement à la protection des données et de la vie privée de ses clients, elle acquiert la réputation de posséder de solides capacités en matière de traitement de l'information. La confiance numérique renforce la confiance dans la marque et, au final, la fidélité des clients.
Négliger les investissements dans des mesures de cybersécurité appropriées peut également avoir un impact négatif sur la croissance d'une organisation. De plus en plus, les entreprises demandent à leurs partenaires potentiels des garanties de cybersécurité. Les gouvernements ont ainsi ajouté des exigences à leurs contrats d'approvisionnement.

Les cyber assureurs étudient les moyens d'évaluer le cyber risque des entreprises et de le lier à la tarification des primes. Les agences de notation des obligations signalent qu'elles vont commencer à prendre en compte la cybersécurité dans leurs analyses, ce qui permettra aux investisseurs d'évaluer de manière tangible la valeur des préparatifs cybernétiques d'une entreprise.

Finalement, la perception de la cybersécurité doit évoluer. Plutôt qu'être perçue comme une contrainte quotidienne, elle doit acquérir le rôle moteur d'innovation pour l'entreprise.

A PROPOS DU CLUB ESSOR INNOVATION

CLUB ESSOR INNOVATION

PARIS&CO

NOTRE MISSION

Accompagner la croissance des PME et ETI en s'appuyant sur la capacité d'innovation des startups et en bénéficiant des retours d'expérience des grands groupes.

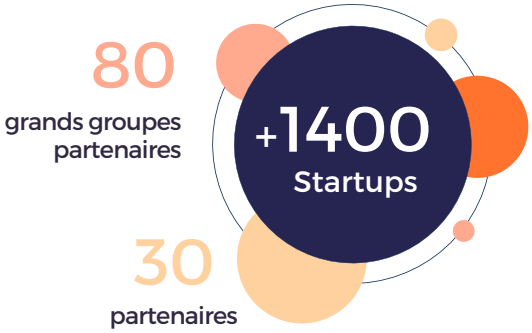
Depuis 2021...

+70 startups impliquées

30 grands groupes contributeurs

20 experts mobilisés

Intégrez la communauté Paris&Co :



80 grands groupes partenaires

30 partenaires institutionnels

250 collaborations entre grands groupes et startups

ILS NOUS ONT DÉJÀ REJOINT

"Nous bénéficions ainsi d'un réseau de milliers de startups et d'experts, d'une veille pointue mais aussi d'une capacité d'innovation décuplée dans des domaines tels quel la data, l'information voyageur, la sécurité, les ressources humaines... nous hissant désormais au niveau des plus grands opérateurs du marché."

Stéphane Guenet, président du Groupement Lacroix & Savac

forum des images · hbs. · AUDITOIRE · GROUPEMENT LACROIX & SAVAC · CHAMBRE DES NOTAIRES DE PARIS

ABVV GROUPE · ECT · CITEO · FITNESS PARK · CENTAURUS HOSPITALITY MANAGEMENT

"L'industrie de la mobilité est en pleine mutation : nous avions besoin d'un regard extérieur pour nous challenger et nous accompagner dans l'élan d'innovation que nous souhaitions insuffler.
Les rencontres avec les différents partenaires, les speed meetings du club, les rendez-vous experts, ainsi que les rendez-vous Paris&Co sont une expérience très riche et intéressante."

Bedros Izikian, Directeur général chez ABVV Groupe

VOS BÉNÉFICES

Une expérience de plus de 10 ans dans l'open innovation

Un parcours et suivi sur-mesure pour atteindre vos objectifs

Un gain de temps pour vos collaborateurs dans la recherche de solutions & expertises innovantes

UN ACCOMPAGNEMENT EFFICACE & PERSONNALISÉ

Le programme associe un ensemble de formats collectifs à une série d'actions individualisées pour :

Identifier les idées et solutions qui vont accélérer votre développement.

Créer les conditions du succès de l'open innovation en adoptant les meilleures pratiques méthodologiques, RH, digitales, rse.

INDIVIDUEL

L'appel à innovation

Identifier les propositions innovantes disponibles ou émergeantes qui vous permettront de renforcer votre offre grâce à un sourcing national.

Le rdv d'expert

Obtenir une réponse personnalisée à vos questions pointues selon vos besoins et objectifs.

COLLECTIF

Le démo day

Découvrir les meilleures solutions innovantes répondant à un enjeu clé partagé.
1h30

L'Atelier

Améliorer sa pratique de l'innovation ouverte.
2h-3h

Le séminaire flash

Disposer d'une veille approfondie sur un sujet stratégique partagé avec les experts de référence.
1/2 journée

La rencontre d'affaires

Ouvrir de nouvelles perspectives de marchés et tester de nouvelles propositions de valeur.

DES EXEMPLES DE CAS D'USAGE

Le besoin ? **Enrichir l'expérience éditoriale et le référencement d'un site d'informations.**

- Organisation d'un challenge startups suivi du test de 3 solutions et du déploiement d'une solution.
  - Site référencé dans le top 3 des moteurs de recherches.

Le besoin collectif ? **Mieux manager à distance et engager des équipes collaborateurs de terrain décentralisées dans le contexte post covid.**

- Élaboration d'un séminaire d'1/2 journée intégrant des intervenants reconnus (experts sciences cognitives, conseils, entrepreneurs) et animation d'un processus de réflexion comm une.
  - Poursuite de la collaboration post-séminaire entre les intervenants et l'entreprise.

INNOVONS ENSEMBLE POUR GAGNER EN PERFORMANCE !

Devenez membre du Club Essor Innovation

Contact
François Tessier, Responsable du Club Essor Innovation
06 80 07 35 99 francois.teyssier@parisandco.com

PARIS&CO

A PROPOS DE PARIS&CO

Paris&Co, organisation d'innovation territoriale, agit pour la transformation durable de la cité. Elle est mobilisée avec et pour les entrepreneurs, convaincue de leur capacité à développer des solutions pérennes pour relever les défis des transitions écologique, économique et sociale.

Paris&Co agit au service de l'intérêt général en acteur indépendant et responsable auprès des opérateurs privés et publics pour faire de l'innovation un levier efficace de transformation. Elle est bâtisseur et opérateur de communautés innovantes.

Paris&Co est un acteur tiers capable de favoriser le dialogue et la production de solutions réalistes et tenables entre toutes les parties prenantes. Elle sait identifier et impliquer les personnes et organisations pertinentes pour analyser, comprendre, expérimenter, déployer des réponses dans une exigence permanente d'impact positif.

Paris&Co s'inscrit dans une perspective de temps long et porte l'ambition du passage à l'échelle pour les entreprises qu'elle accompagne et les projets d'innovation qu'elle contribue à développer.

Paris&Co est une organisation locale d'impact national et international qui contribue à faire rayonner Paris et sa métropole comme territoire porteur d'innovation utile et positive.

www.parisandco.paris

Directeur de publication :
Loïc Dosseur, Directeur Général de Paris&Co

contactpresse@parisandco.com

Rédaction et conception :
François Teyssier, Responsable du Club Essor Innovation
Paula Bouquet, Chargée de Communication et Evènementiel

Graphisme et mise en page :
Camille Laurella

CLUB ESSOR INNOVATION

PARIS&CO