vtx TELECOM

La Cybersécurité n'est plus une option

Auteurs : B. Vicari - P. Mundwiller - C. Duffour

SOMMAIRE

Pourquoi ce livre blanc ?

Comme la plupart des dirigeants et des cadres d'entreprises, vous placez la sécurité de vos infrastructures au cœur de vos préoccupations et vous avez raison. Le travail à distance s'est généralisé, intensifiant d'autant les opportunités de cyberattaques, à un point tel que les cybercriminels n'épargnent plus rien, ni personne.

Aujourd'hui, pour les groupes de hackers, vos données informatiques ont plus de valeur que le pétrole ou l'or et la probabilité que votre organisation soit un jour la cible d'une attaque d'envergure est proche de 100 %.

Face à ces nouvelles cybermafias, une entreprise, quelles que soient sa taille et la qualité de son architecture défensive, ne peut plus espérer se protéger seule. Les pirates ne dormant jamais, le graal serait de pouvoir veiller vos avoirs informatiques 24/7.

Un tel niveau de cybersécurité existe.

On le trouve au sein d'un Security Operation Center, un SOC. Jusqu'à présent, ces services de cyberdéfense haut de gamme étaient réservés à des états, des grandes institutions ou à de grosses multinationales. Jusqu'à présent.

Car la pratique se démocratise. De plus en plus d'entreprises et de collectivités vont pouvoir bénéficier des services d'un centre des opérations de sécurité.

Mais commençons par le commencement...

Pierre Marty
CEO VTX TELECOM

HACKER **OUVERT**

Hacker. Ce mot qui fait peur est apparu pour la première fois dans les années 50 au Massachusetts Institute of Technology de Boston, le célèbre MIT.

« Hack » désigne alors un mélange de délire créatif et d'exploration sans limite, de blagues potaches et d'ingénieuse bricole. On parle des « spéléo-hackers » pour qualifier les étudiants intrépides qui sondaient les égouts et les conduits de ventilation de l'université.

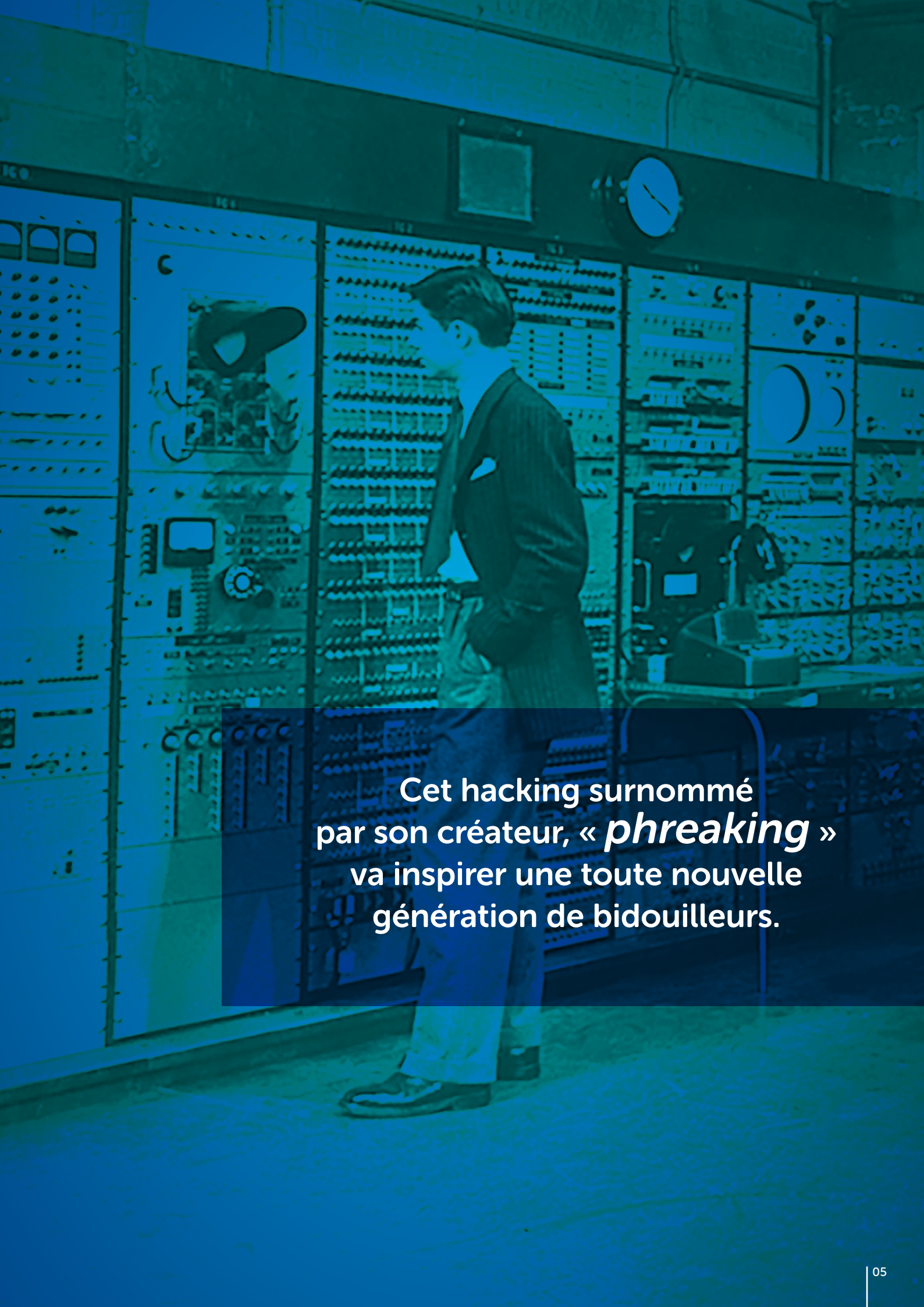
Les membres du club de modélisme du MIT furent sans doute les premiers à se désigner comme des « hackers », après avoir réussi à piloter un circuit de petits trains à distance grâce à un téléphone. Un petit pas pour l'homme...

A la fin des années 1950, le titre de hacker est donc un signe de reconnaissance. Il est celui qui se distingue par ses prouesses techniques, sa malice et l'originalité de la solution qu'il apporte à un problème.

En 1969, un certain John Draper trouve un sifflet cadeau dans une boite de céréales. Il découvre bientôt que l'objet possède la même tonalité que le réseau téléphonique américain et il parvient à passer des appels longue distance gratuitement en sifflant dans le combiné. Astucieux, mais illégal...

Cet hacking surnommé par son créateur, « phreaking » va inspirer une toute nouvelle génération de bidouilleurs.

Aujourd'hui encore, un hacker désigne un virtuose pouvant intervenir dans différents domaines comme la programmation, l'architecture matérielle d'un ordinateur, l'administration système, l'administration réseau, la sécurité ou tout autre domaine de l'informatique.



Cet hacking surnommé
par son créateur, « *phreaking* »
va inspirer une toute nouvelle
génération de bidouilleurs.

Tous les hackers ne servent pas les mêmes causes et on a pris l'habitude de les classer en trois catégories : les blancs, les noirs et les gris.

Un « Black Hat » est une personne qui recherche et exploite malicieusement les vulnérabilités des systèmes ou des réseaux informatiques, en utilisant, dans le but de nuire, des logiciels malveillants et d'autres techniques de piratage. Ces criminels d'un nouveau genre enfreignent les lois, infiltrant les réseaux de leurs victimes à des fins lucratives, pour voler ou détruire des données, pour perturber les systèmes, pour faire du cyber-espionnage ou simplement, mais c'est de plus en plus rare, pour s'amuser.

A l'autre extrémité, un « White Hat » est un spécialiste de la sécurité engagé pour trouver des vulnérabilités dans les logiciels, le matériel et les réseaux qui sont autant de terrains de chasse pour les cybercriminels. Contrairement aux « Chapeaux Noirs », les « Chapeaux Blancs » ne piratent les réseaux que lorsqu'ils sont légalement autorisés à le faire.

Egalement connus sous le nom de « hackers éthiques », les « White Hats » divulguent toutes les vulnérabilités à leur employeur et au fournisseur dont le matériel ou le logiciel est affecté, afin qu'ils puissent appliquer un correctif aux systèmes fragilisés. Les techniques de piratage des chapeaux blancs comprennent les tests de pénétration et les évaluations de vulnérabilité.

Comme les choses ne sont jamais noires ou blanches, il existe aussi des « Grey Hats ».

Ils exploitent les failles de sécurité sans intention malveillante, comme les « Chapeaux Blancs », mais ils peuvent utiliser des méthodes illégales pour trouver ces failles.

Même si leurs intentions sont pacifiques, les hackers « Chapeaux Gris » vont souvent identifier des faiblesses et pirater des systèmes sans la permission de leur cible. Certains vont même jusqu'à divulguer ces failles de sécurité au grand public ou vendre des informations pour en tirer un bénéfice, comme le ferait un « Chapeau Noir ».

AVIS D'EXPERT

Derrière le terme générique de « pirate » se dissimulent de multiples acteurs malveillants comme les organisations criminelles, des hacktivistes ou des espions d'Etats. Leurs objectifs vont d'une simple satisfaction personnelle à des enjeux géopolitiques ou gains financiers.

Les « White Hats » divulguent toutes les vulnérabilités, afin d'appliquer un correctif aux systèmes fragilisés.

LE NOUVEAU FAR WEST

Dans ce nouveau monde interconnecté, face à la multiplication des menaces et la montée en puissance des gangs de cybercriminels, la cybersécurité doit devenir une priorité, presque une obsession pour tous les chefs d'entreprise qui ne veulent pas voir leurs efforts et leur réputation ruinés par un clic de souris sur un fichier piégé.

En 2021, on a recensé dans le monde, une cyber-attaque toutes les 39 secondes et 2300 incidents ont été signalés en moyenne par jour.

Plus inquiétant encore, les pirates élargissent leur champ d'action à des domaines qui jusque-là avaient été relativement épargnés, comme le secteur de la santé ou des PME.
L'histoire retiendra que le premier décès officiellement causé par une cyber-attaque est survenu en septembre 2020, lorsqu'une intrusion par ransomware (rançongiciel) a provoqué une panne informatique dans un hôpital de Düsseldorf, en Allemagne.

Toujours en 2020, plus de la moitié des cyber-attaques mondiales ont été commises contre des petites et moyennes entreprises.

Les PME semblent être devenues une cible de choix pour les hackers, car elles sont en général moins bien protégées que les grandes entreprises ou les multinationales qui ont les moyens de construire des architectures numériques solides, capables d'offrir de réelles garanties en termes de protection et de fiabilité des données.

La cybersécurité, soit l'ensemble des mesures prises pour protéger les valeurs d'une entreprise n'est plus une option. La bonne question à se poser n'est pas : « que vais-je faire si je suis attaqué ? » mais : « que vais-je faire quand je serai attaqué ? »

> ***En 2020, plus de la moitié des cyber-attaques mondiales ont été commises contre des petites et moyennes entreprises.***

Les menaces peuvent être multiples et vicieuses, massives ou invisibles. Ce sont souvent des attaques externes qui portent des noms que vous connaissez, phishing, malware et ransomware.

Le phishing

Le phishing est un cybercrime qui consiste à utiliser de faux mails, sites Web et messages textes incitant la victime à révéler des informations personnelles ou corporatives confidentielles, exploitées par la suite par des criminels pour des vols d'identité. Cette technique est également utilisée pour rendre les ordinateurs vulnérables à l'introduction d'un logiciel malveillant.

Le malware

Le malware désigne une grande variété de logiciels intrusifs utilisés par les hackers pour pénétrer dans le réseau informatique d'une société et y soustraire des informations sensibles. Le cheval de Troie se dissimule derrière des logiciels pour créer des brèches par lesquelles les cybercriminels peuvent entrer et se servir. Les pirates peuvent aussi prendre le contrôle de votre machine à distance et l'utiliser avec des milliers d'autres pour engendrer des attaques informatiques massives.

Le ransomware

Le ransomware est un outil employé par les pirates pour gagner beaucoup d'argent. Il se présente sous la forme d'un logiciel malveillant ou d'un virus qui bloque l'accès à l'ordinateur et à ses fichiers et réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. C'est l'attaque idéale pour cibler une entreprise. Avec la multiplication des attaques par ransomware, une nouvelle profession a fait son apparition : le cybernégociateur. Il est très souvent appelé en urgence par des entreprises victimes d'une prise d'otage de leurs données digitales et il doit tenter de limiter les dégâts et de minimiser la rançon en utilisant des méthodes aussi bien techniques que psychologiques, à la limite de la légalité.

AVIS D'EXPERT

Les attaquants s'adaptent à l'actualité ; typiquement durant la COVID-19 une recrudescence d'E-mails de phishing sur le sujet de la santé a été observée et utilisée pour propager des ransomwares. En 2021, 58 % des victimes de ransomwares ont payé la rançon. La rançon moyenne demandée en 2021 est de 250 000 USD.

TOUS VISÉS

Par le passé, les petits poissons n'avaient pas à s'inquiéter disait-on. Les temps ont radicalement changé. Toutes les entreprises petites, moyennes, grandes, très grandes sont aujourd'hui susceptibles de subir une importante violation de leurs systèmes informatiques reliés à l'Internet.

En 2021 au Canada, 86 % des organisations ont été victimes de cyber-attaques avec un taux de réussite pour les pirates de presque 6 %. Les criminels, qui ratissent au chalut des océans de données, ne savent pas toujours ce qu'ils cherchent, mais ils savent, en revanche, très bien exploiter ce qu'ils trouvent.

Donc, un beau jour, ou peut-être une nuit, votre entreprise sera la cible d'une attaque aux conséquences désastreuses pour vos finances et votre réputation.

Les victimes sont souvent des sociétés qui ne disposent pas des personnes et des ressources nécessaires pour atténuer les risques d'une attaque en mettant en place une défense « en profondeur ».

Prévenir
Détecter
Récupérer

voilà la marche à suivre.

Aujourd'hui, prévenir votre entreprise d'une cyber-attaque implique l'installation d'outils, la mise en place d'infrastructures et l'utilisation de services qui doivent converger vers un seul but : empêcher les cybercriminels d'accéder à vos données !

Cependant, malgré les efforts déployés pour prévenir les attaques, certaines parviendront quand même à tromper vos défenses primaires. Il est donc essentiel de les détecter rapidement et de les éliminer ou, au moins, de les contenir.

Si malgré toutes ces précautions, les pirates pénètrent dans vos réseaux, infectent et neutralisent vos infrastructures, il faut encore être capable de récupérer vos données, ce qui implique l'utilisation d'un système de sauvegarde suffisamment sophistiqué pour faire un copié/collé de la totalité de vos avoirs informatiques perdus.

« Les criminels, qui ratissent au chalut des océans de données, ne savent pas toujours ce qu'ils cherchent. »

Les bandes de cybercriminels sont très bien organisées, elles sont gérées comme des entreprises et souvent pilotées par des Etats. Ces criminels engrangent des centaines de millions de dollars en piratant des serveurs ou des réseaux et en exigeant des rançons. Mais rassurez-vous, rien de personnel, car les hackers utilisent des outils automatisés sophistiqués qui frappent à la porte de tout le monde !

AVIS D'EXPERT

Les pirates sont toujours à l'affût des failles de sécurité et prêts à sauter sur des opportunités d'attaque sur les entreprises de toutes tailles et tout secteur d'activité. Plus de 70 % des entreprises ciblées au niveau mondial ont moins de 1000 employés.

DU CHÂTEAU FORT À L'OIGNON

Il y a longtemps qu'on ne conçoit plus la sécurité d'une entreprise comme une grosse place forte entourée d'une épaisse muraille digitale censée repousser les pirates.

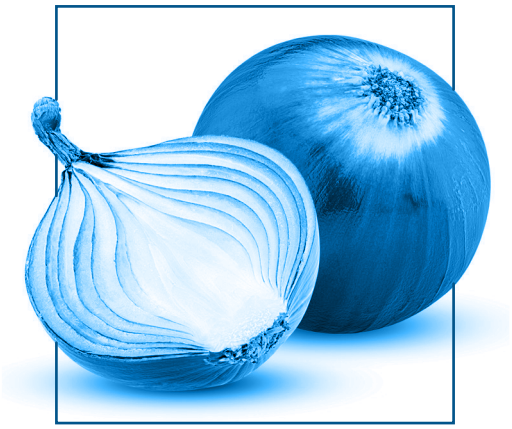
Les méthodes de cyber-attaque évoluent constamment. Il devient indispensable d'assurer une surveillance constante de vos infrastructures et surtout de mettre en place une défense à plusieurs niveaux. L'idée est aussi simple qu'elle en a l'air : au lieu de n'avoir qu'une seule couche de sécurité, vous en intégrez plusieurs. Et, pour les hackers, réussir à attaquer un oignon devient tout de suite plus compliqué.

Couche de sécurité des données

Vos données sont sans doute votre bien le plus précieux. Les systèmes d'exploitation et les applications peuvent être restaurés, mais ce n'est pas toujours le cas des données originales.

Il faut donc régulièrement sauvegarder les données concernant votre entreprise, vos états financiers et bien sûr, les données de vos clients. Régulièrement signifie tous les jours et parfois même toutes les heures !

La sauvegarde de données va crypter et copier l'ensemble de vos fichiers sur un système sécurisé, hors site. Les sauvegardes sont conservées de manière chronologique. Cela veut dire que vous pourrez restaurer vos données passées à n'importe quel moment, par exemple, avant l'arrivée d'un virus. Votre entreprise pourra alors reprendre ses activités en quelques heures, au lieu de quelques jours ou semaines.



AVIS D'EXPERT

La sécurité à 100 % n'existe pas. Il est important d'avoir un système de défense qui en tienne compte. Par exemple, le simple vol d'un mot de passe ne doit pas permettre un accès à l'entreprise depuis Internet. Un deuxième niveau de contrôle avec smartphone ou SMS est nécessaire pour une bonne protection des accès à distance.

SÉCURITÉ DU RÉSEAU

Les réseaux informatiques internes sont l'une des principales cibles d'attaques car leur conception, souvent obsolète, n'intègre que très rarement la prise en compte des risques sécurité. Cela se manifeste généralement par une absence de dispositifs et de procédures de gestion des accès et l'utilisation de mots de passe simples, beaucoup trop faciles à pirater.

SÉCURITÉ DES POINTS FINAUX

La protection des points finaux fait référence à la protection des réseaux qui sont reliés à distance à vos appareils, comme votre ordinateur portable, votre tablette et votre téléphone mobile. La connexion de ces appareils à l'extérieur va ouvrir des boulevards pour les menaces de sécurité, surtout si en déplacement vous utilisez du wifi public.

SÉCURITÉ DES APPLICATIONS

Il est possible de piloter la sécurité de son écosystème applicatif de manière totalement centralisée afin de pouvoir l'adapter progressivement et de manière agile aux règles de conformités. Pour ce faire, il est fortement recommandé d'intégrer, dès la conception, des APIs (interfaces de programmation applicative) permettant un meilleur contrôle des fonctions sensibles de vos applications.

SÉCURITÉ ET IDENTIFICATION DES ACCÈS PHYSIQUES

Certaines mesures ne sont pas à négliger pour garantir une couche de sécurité matérielle à votre environnement professionnel. Avez-vous installé des caméras surveillant vos accès à l'extérieur ? Vos collaborateurs sont-ils badgés ? Votre wifi visiteurs est-il sécurisé ? Qui a accès à votre centre IT ? Votre entreprise est-elle divisée en zones réservées ?

SÉCURITÉ DU COURRIER ÉLECTRONIQUE

La sécurité du courrier électronique doit être une priorité pour toutes les entreprises. Des recherches ont montré que 9 virus sur 10 qui infectent les ordinateurs proviennent d'une pièce jointe à un courriel. Il s'agit donc d'un domaine vital à protéger. Veillez à utiliser un bon filtre anti-spam et à analyser les pièces jointes. Pour une protection supplémentaire, le cryptage peut assurer la confidentialité des E-mails en préservant la sécurité des données et des messages entre l'expéditeur et le destinataire.

PRÉVENIR POUR MIEUX GUÉRIR

Personne n'aime les problèmes et encore moins les mauvaises surprises. Ouvrir son ordinateur un matin pour se retrouver face à un masque blanc à moustache vous réclamant une énorme rançon en bitcoin n'est pas la meilleure façon de commencer une journée de travail.

Affronter une menace c'est d'abord admettre qu'elle existe. Vous allez donc devoir faire le premier pas, adopter une posture de défense active et commencer par une évaluation lucide de la protection actuelle de vos systèmes informatiques.

VOUS ÊTES-VOUS DÉJÀ POSÉ CE GENRE DE QUESTIONS ?

- Utilisez-vous un antivirus professionnel ?
- Avez-vous activé un pare-feu ?
- Sécurisez-vous votre messagerie électronique ?
- Avez-vous implémenté une politique de mots de passe robustes ?
- Connaissez-vous vraiment votre parc informatique et ses interconnexions avec l'extérieur ?

- Effectuez-vous des sauvegardes et des mises à jour régulières ?
- Savez-vous où se trouvent ces sauvegardes ?
- Acceptez-vous l'usage des réseaux sociaux professionnels ou non ?
- Avez-vous fixé les droits de chacun de vos collaborateurs et savez-vous vraiment qui a accès à quoi ?
- Informez-vous et sensibilisez-vous régulièrement vos collaborateurs aux risques de cyber-attaques ?

- Maîtrisez-vous votre sécurité numérique lors des missions et des déplacements professionnels ?
- Avez-vous établi une charte d'utilisation informatique en externe avec vos prestataires et fournisseurs ?
- Avez-vous établi une charte de sécurité interne signée par vos collaborateurs ?
- Avez-vous fait tester votre système de défense par des spécialistes ?
- Savez-vous comment réagir en cas de vraie cyber-attaque ?

- Etes-vous prêt à payer une rançon pour récupérer vos postes de travail ?
- Etes-vous prêt à fermer votre entreprise pendant une semaine ou un mois ?
- Etes-vous prêt à perdre des clients quand leurs datas auront filtré sur le dark web ?
- Avez-vous fait évaluer la couverture de votre police d'assurance au cyber-risque ?

Si vous avez répondu honnêtement à toutes ces questions et que vous avez le sentiment d'avoir encore quelques trous dans la raquette, c'est tout à fait logique.

Le monde de la cybersécurité est devenu si complexe qu'il ne peut pas être appréhendé par une entreprise seule, même si elle est dotée d'un département IT et sécurité compétent.

Cependant, entreprendre la construction d'un écosystème cybersécuritaire complet, efficace et résilient requiert des moyens importants et des compétences très spécifiques jusqu'à présent hors de portée de la plupart des sociétés.

C'est pourtant la meilleure voie à suivre. Mais cela implique de pouvoir démocratiser l'usage d'outils et de services extrêmement performants qui étaient jusqu'à présent réservés à des Etats, des institutions financières ou à de grandes multinationales.

A ce niveau de surveillance, les menaces sont anticipées, contrées ou confinées par des professionnels aguerris capables, 24/24 et 7/7, de scanner la totalité du réseau Internet mondial pour détecter et répondre en temps réels aux potentielles attaques ciblant votre entreprise ou votre branche d'activité.

Ce service de cybersécurité premium porte un nom ou plutôt un acronyme, le SOC.

AVIS D'EXPERT

La plupart des attaques capitalisent sur les périodes de faible vigilance pour lancer leurs offensives. Typiquement, il est fréquent de détecter le démarrage d'attaques informatiques le vendredi en fin de journée, juste avant un long week-end ou durant des périodes de vacances d'où l'intérêt d'un système de cyberdéfense 24 h sur 24.

AIDE-TOI ET LE SOC T'AIDERA

Aujourd'hui, une organisation qui ne dispose pas de processus clairs pour identifier, signaler et répondre à un incident de cybersécurité, risque de le payer très cher.

Le SOC, ou le Security Operation Center, représente la première couche d'une infrastructure sécuritaire en forme d'oignon. C'est un service spécialisé qui va permettre à une entreprise de surveiller, administrer et sécuriser en temps réel 24/7 son réseau et ainsi réduire considérablement les risques et les menaces informatiques.

Installer et exploiter un SOC privé n'en demeure pas moins un exercice très compliqué.

Un centre opérationnel de sécurité performant requiert en effet l'utilisation de technologies de pointe mais aussi l'engagement de spécialistes aux profils très particuliers. Les entreprises doivent avoir de très bonnes raisons pour le mettre en place.

La construction d'un SOC est donc souvent l'apanage des nations, d'importantes multinationales ou de grandes sociétés privées spécialisées dans la cybersécurité.

Maintenir une cybersécurité forte demande beaucoup d'investissements. Un SOC centralisé permet à une entreprise de réduire ses coûts en les partageant avec d'autres organisations. Peu à peu, la pratique se démocratise et de plus en plus d'entreprises vont pouvoir bénéficier des services d'un Security Operation Center.

Comme chez le docteur.

Dans un premier temps, le SOC va évaluer l'ensemble des risques auxquels votre organisation est confrontée et ausculter ses infrastructures et ses processus critiques. Une fois cet audit général effectué, le SOC pourra en déduire les vulnérabilités et les menaces pesant sur votre système. Les risques devront être classés en fonction de leur degré de dangerosité.
Des simulations de cyber-attaques, appelées pen-testing, seront aussi réalisées par des « Chapeaux Blancs » afin de trouver les failles, les mauvaises configurations du système et évaluer l'efficacité de la solution mise en place par votre entreprise.

Pour finir, une fois les failles détectées, un plan d'action est proposé visant à diminuer la vulnérabilité des systèmes. Le SOC va aussi inciter l'entreprise à obtenir des certifications et l'aider à mettre en place des procédures d'urgence que les employés devront suivre en cas d'incident.

Grâce à la surveillance des forums pirates, du web et du dark web, à l'utilisation d'algorithmes et de l'intelligence artificielle, un SOC peut anticiper, voire prévenir les attaques, et agir pour votre entreprise comme le ferait un ange gardien, 24 heures sur 24 et 365 jours par an, car les pirates ne dorment jamais.

Si on part du principe qu'une violation de données ou une attaque par ransomware peut rapidement vous coûter des millions, un SOC qui bloque ne serait-ce qu'une seule intrusion avant que des dommages irrémédiables ne soient causés représente déjà un retour sur investissement significatif.

> ***Mauvaise nouvelle, les cyber-attaques sont de plus en plus nombreuses. Bonne nouvelle, vous n'allez pas les affronter seul.***

AVIS D'EXPERT

La planification du système de défense doit se baser sur les risques réels auxquels font face les entreprises comme le blocage des systèmes par un ransomware, le vol de données ou l'indisponibilité d'un site d'e-Commerce. Une bonne planification va permettre une réaction précise et efficace qui limitera l'impact sur les affaires en cas d'incident.

LE MAILLON FAIBLE

Vous voilà bien protégé.

Vous avez mis toutes les chances de votre côté, vos infrastructures sont hautement sécurisées, votre réseau a été testé, vos logiciels mis à jour, votre entreprise est certifiée et vos procédures bien en place car vous disposez d'un service de SOC qui veille jour et nuit sur vos avoirs numériques.

Vous pensez pouvoir dormir tranquille ? Pas encore...

De tous les paramètres à prendre en compte pour renforcer la sécurité d'une organisation, le facteur humain est de loin le plus important. Le chiffre est terrible mais 90 % des attaques pirates réussissent à cause d'une « erreur » humaine. En résumé, le ver est dans l'oignon.

Vos collaborateurs peuvent à n'importe quel moment révéler des informations sensibles en cliquant sur un simple fichier joint. Ils peuvent aussi répondre à un courriel de leur chef de service qui n'est, en fait, pas envoyé par leur chef de service... Les pirates sont très créatifs et nous sommes souvent trop crédules.

Nous nageons de fait, en plein paradoxe. La totalité des employés d'une entreprise savent comment réagir quand ils entendent une alarme incendie et beaucoup pourront se servir efficacement d'un extincteur. D'autres auront des notions de premiers secours ou sauront qui appeler en cas de malaise d'un collègue au bureau. Parce que ce sont des réflexes sécuritaires collectifs ancrés dans la culture des sociétés modernes.

Il devrait en être de même pour la cybersécurité.

Permis de surfer.

S'il est essentiel d'armer vos équipes de connaissances pratiques pour prévenir les violations, il est aussi important de développer une culture de responsabilité et de vigilance collective afin de limiter au maximum les risques de cyber-intrusion.

Une chartre de cybersécurité, signée par vos collaborateurs, incluant bons usages et procédures d'urgence est le socle incontournable sur lequel toute entreprise doit construire sa première ligne de défense interne.

Pour pouvoir conduire une voiture ou une moto en toute sécurité, il faut d'abord passer un permis. Cela semble logique. Pour sillonner les autoroutes de l'information aux commandes de sa souris, il faudrait un permis aussi. Ce n'est peut-être qu'une question de temps.

Pensez-y.

La sensibilisation et la formation des utilisateurs finaux aux cybermenaces sont devenues indispensables à la sécurité des entreprises qui les emploient.

CONCLUSION DE L'EXPERT

Environ 50 % des attaques ciblent directement les utilisateurs informatiques par des E-mails frauduleux. Nos équipes de réponse aux incidents sont régulièrement engagées sur des cas d'ampleur importante qui ont démarré par un simple E-mail à un utilisateur. Cela souligne la responsabilité de chaque utilisateur dans le système de cyberdéfense.

Aujourd'hui, la cybersécurité doit être considérée comme un investissement pour une organisation.


vtx
TELECOM
www.vtx.ch
0800 200 200