LA MENACE EST RÉELLE

RISQUES ACTUELS ET FUTURS AU SEIN D'UNE ENTREPRISE

Les entreprises suisses sont exposées en permanence à des menaces numériques. La qualité et l'ampleur des cyberattaques, qu'elles soient le fait de petits délinquants ou de pirates informatiques bien organisés, ne cessent d'augmenter. Les entreprises de taille moyenne, en particulier, ne sont pas conscientes de ce risque. Elles supposent qu'elles sont trop petites ou trop peu connues pour représenter un quelconque intérêt pour les pirates. Cependant, elles sont depuis longtemps devenues une cible potentielle des hackers.

« Il existe deux types d'entreprises : celles qui ont été piratées et celles qui ne le savent pas encore ». Cette affirmation est devenue le mot d'ordre des experts en sécurité. En Suisse, le rapport intitulé « The CYBER RISK SURVEY REPORT 2018, cyber risk from a Swiss perspective », rédigé par KESSLER & CO Inc., montre la gravité de la situation : à la question de savoir si leur entreprise avait été victime d'une cyberattaque au cours des 12 derniers mois, 66 % des participants ont répondu par « non », 24 % par « oui » et 10 % par « je ne sais pas ». À cet égard, on peut supposer qu'une partie des 66 % des entreprises qui ont répondu « non » n'ont pas encore découvert que leur entreprise a été piratée. En effet, les logiciels malveillants ne sont souvent détectés qu'après plusieurs semaines ou mois, voire pas du tout.

Derrière ces attaques se cachent des groupes organisés de hackers. Ces derniers utilisent des méthodes de plus en plus sophistiquées qui donnent du fil à retordre aux entreprises. On oublie cependant que de nombreux cybercriminels ne sont pas aussi bien équipés d'un point de vue technique que les hackers professionnels : ils exploitent tout simplement des failles de sécurité facilement évitables ainsi que les comportements insouciants. Toute trace de négligence lors de l'installation d'une mise à jour de sécurité ou du système d'exploitation, les configurations inadéquates, les mots de passe peu sécurisés et les employés qui ouvrent des pièces jointes dont l'origine n'a pas été vérifiée, en toute connaissance de cause, représentent des accès au réseau de l'entreprise pour le hacker. Une fois entré dans le réseau, il essaiera d'accéder à des comptes disposant de plus de droits, comme les comptes d'administrateurs, de serveurs ou de bases de données afin de rechercher des informations sensibles.

Bien que la cybercriminalité soit devenue un sujet omniprésent, de nombreuses entreprises de taille moyenne n'ont pas conscience qu'elles sont exposées aux cyberattaques. Les *Hidden Champions* (champions cachés, il s'agit une expression qui désigne des petites entreprises discrètes, mais leaders sur leur marché) sont la cible de prédilection des pirates informatiques en raison de leurs compétences et brevets. Néanmoins, la taille de l'entreprise n'est en rien un facteur déterminant dans le cas de cyberattaques de masse, non ciblées, telles que les tentatives de *phishing* (hameçonnage). Au contraire : plus une entreprise est petite, plus les chances de succès sont élevées pour le hacker en raison du budget plus limité alloué à la sécurité informatique et du manque de personnel spécialisé en la matière.

En effet, les mesures de sécurité traditionnelles ne suffisent plus à se protéger de la cybercriminalité. Ce livre blanc vous présente les dangers potentiels actuels et futurs à l'aide d'exemples.

Dangers liés à la chaîne d'approvisionnement en logiciels

Les attaques visant la chaîne d'approvisionnement, c'est-à-dire la coopération, la communication et les échanges avec les fournisseurs, prennent de plus en plus d'ampleur à l'échelle mondiale. Selon une étude de l'institut Ponemon publiée en décembre 2018, 56 pour cent des entreprises ont subi une violation de la protection de leurs données par un de leurs fournisseurs. Seuls 35 pour cent des participants à l'enquête ont pu, par ailleurs, dresser une liste exhaustive des partenaires avec lesquels des informations sensibles ont été partagées. La chaîne d'approvisionnement des logiciels pose un problème supplémentaire : les moyens permettant d'infiltrer des logiciels réellement fiables s'étendent de la compromission de progiciels libres à la fourniture d'une mise à jour affectée par un logiciel malveillant. Le cheval de Troie « NotPetya », par exemple, s'est vraisemblablement répandu en 2017 sous la forme d'une mise à jour d'un logiciel de gestion en passant par un serveur piraté. Le ransomware a infecté aussi bien les grandes entreprises que les petites et a engendré des pertes qui se comptent en millions.

Si un hacker parvient à prendre le contrôle du firmware, c'est-à-dire le programme qui fait le lien entre le matériel et le système d'exploitation, toutes les mesures de sécurité installées par la suite deviennent pratiquement inutiles. Par conséquent, les entreprises doivent acheter

SYSTÈME D'EXPLOITATION OBSOLÈTE : UNE INVITATION POUR LES HACKERS

Selon une analyse récente du fournisseur de logiciels de sécurité Kaspersky Labs, le système d'exploitation agit comme une bombe à retardement pour de nombreuses entreprises. Plus de la moitié des entreprises de taille moyenne utilise un système d'exploitation obsolète ou qui ne sera bientôt plus pris en charge, comme Windows XP ou Windows 7. Cependant, les failles de sécurité non corrigées constituent une porte d'entrée très appréciée des cybercriminels.

du matériel et des logiciels qui ne proviennent que de fournisseurs fiables qui procèdent à des contrôles de sécurité et de conformité exhaustifs. Parallèlement, elles doivent contrôler de manière stricte les accès au réseau de l'entreprise de chaque fournisseur ou partenaire et les zones qui leur sont accessibles.

Le facteur de risque le plus important est et reste l'Homme

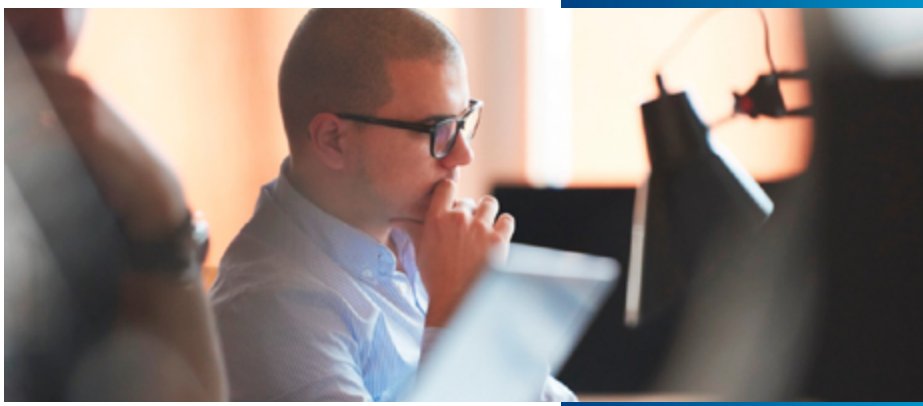
Les failles de sécurité pour lesquelles les criminels misent sur l'imprudence humaine sont en tête de liste. Outre les logiciels malveillants classiques, les e-mails de phishing sont une méthode très appréciée des hackers. Grâce à des sites Internet factices ou à des pièces jointes apparemment inoffensives, ces courriers permettent d'introduire des ransomwares dans le réseau de l'entreprise. Une société s'expose également à des risques si les employés téléchargent d'eux-mêmes une mise à jour de programme sans faire attention au site web d'où provient le fichier. Les méthodes utilisant l'Internet ne sont néanmoins pas les seules à être utilisées dans l'ingénierie sociale : une intervention urgente peut être demandée par téléphone, par exemple, pour un prétendu problème de réseau, bien entendu fictif, afin que la personne appelée divulgue ses données de connexion. Autre exemple : le « patron » aurait apparemment demandé que vous lui transmettiez des informations importantes. Cette méthode ayant recours à l'autorité se voit très souvent couronnée de succès.

Il est par conséquent d'autant plus important que la cybersécurité fasse partie intégrante des directives internes de l'entreprise. L'ensemble du personnel doit être impliqué dans la mise en place de nouveaux systèmes, se familiariser avec les stratégies de sécurité et être sensibilisé aux dangers que représente l'ingénierie sociale. De plus, il est recommandé aux entreprises de segmenter leur réseau et de définir clairement les droits d'accès de chacun. En procédant de la sorte, les criminels qui obtiennent un accès moins privilégié ne peuvent pas pénétrer immédiatement dans l'ensemble du réseau de l'entreprise.

Déplacement des données vers la périphérie du réseau grâce à la 5G et au cloud

Comment les entreprises peuvent-elles protéger leurs données lorsque de plus en plus d'entre elles sont déplacées vers la périphérie du réseau ou vers le cloud ? Les entreprises doivent se poser cette question dès maintenant, car cette problématique est vouée à gagner en pertinence dans les années à venir. En effet, grâce à la 5G, de plus en plus d'appareils, capteurs et services critiques seront connectés les uns aux autres par le biais du réseau et de plus en plus d'environnements OT *(Operational Technology,* technologie d'exploitation) fusionnent avec l'informatique en raison de l'Internet des objets. Cette situation accroît le nombre de points d'attaque potentiels pour les hackers, qui peuvent alors, dans le pire des cas, utiliser le réseau de l'entreprise pour accéder à des données précieuses relatives à la propriété intellectuelle, aux finances et à la clientèle.

Les infrastructures OT présentent généralement une particularité : les cycles de vie du matériel utilisé pour les installations industrielles sont généralement compris entre 20 et 30 ans.



De plus, il est impossible de procéder aux travaux de maintenance durant la nuit comme il est de coutume pour l'informatique classique, car les réseaux OT sont conçus pour fonctionner en permanence, de jour comme de nuit. Dans ce contexte, il est bien entendu difficile de procéder à une mise à jour des mécanismes de sécurité et les correctifs ne fonctionnent souvent pas. Cette faille de sécurité doit être

corrigée à l'avenir. En outre, les méthodes traditionnelles basées sur des éléments de sécurité non corrélés et non connectés ne seront pas en mesure de détecter les attaques et d'y mettre un terme dans les réseaux 5G.

Le franc succès du cloud signifie également que les entreprises doivent garder un œil sur les données et sur les risques potentiels de sécurité et de violation de la protection des données qui y sont associés. Dans quelques années, le multicloud s'imposera comme norme. À l'instar d'une entreprise quelconque, les fournisseurs de services de cloud ne sont pas à l'abri d'une cyberattaque. Par conséquent, les entreprises doivent choisir leur fournisseur avec soin et prêter attention aux certificats, aux délais de disponibilité et aux services additionnels. Outre l'aspect sécurité, les exigences de conformité, telles que le RGPD, jouent également un rôle décisif dans les situations de cloud computing. Le niveau de sécurité des données proposé par le service de cloud sélectionné doit toujours correspondre aux risques associés au traitement de données personnelles.

Un poste vacant est une porte d'entrée pour les criminels

Le manque d'experts en informatique et en sécurité, que de nombreuses entreprises ressentent déjà aujourd'hui, s'accentuera dans les années à venir et deviendra ainsi le meilleur allié des cybercriminels. Afin d'attirer davantage de jeunes issus de ce domaine, les conditions-cadres doivent être améliorées à un stade très précoce. Pour cela, il peut être judicieux de prendre exemple sur d'autres pays. Prenons l'exemple de l'Estonie : son système scolaire intègre des « cours de cybernétique ». En Grande-Bretagne, la programmation est une matière obligatoire pour tous les écoliers à partir de cinq ans. Dans le cadre de leur cours de TIC (Technologies de l'information et de communication), ils apprennent à comprendre les processus, à développer une pensée logique et à élaborer des algorithmes. Ils mettent ainsi un pied dans le monde du travail numérique à un stade précoce de leur vie d'adulte. A contrario,

en Suisse, l'informatique doit se développer et s'imposer davantage dans les cursus scolaires afin d'enseigner d'une part le maniement des technologies de l'information et des télécommunications actuelles et futures, et d'autre part des connaissances de base en matière de cybersécurité.

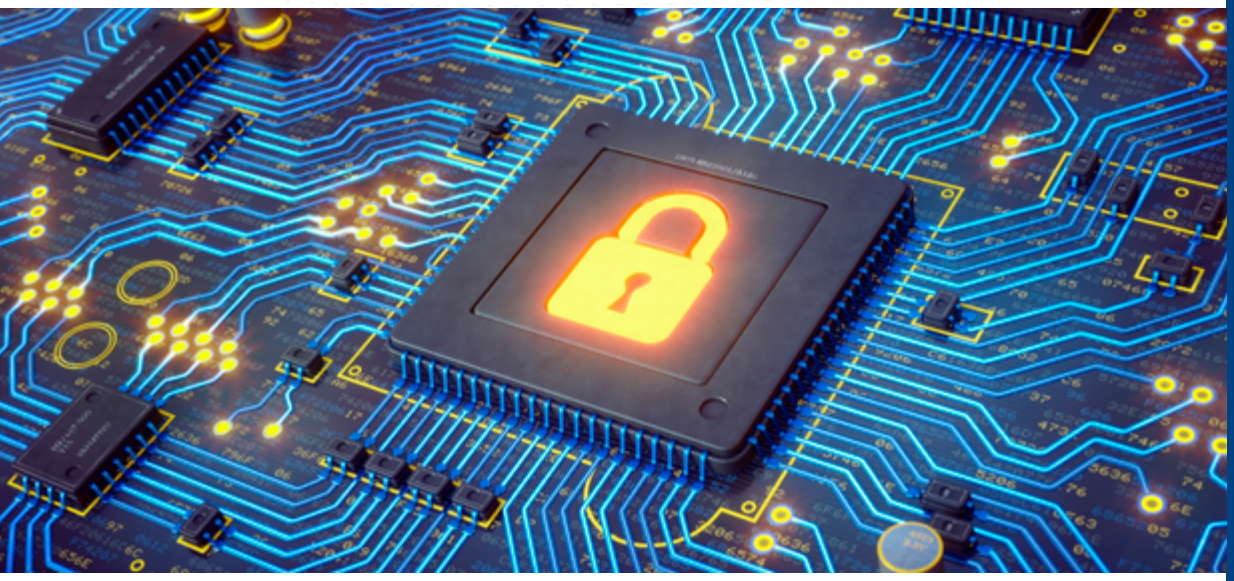
Toutefois, en raison de la durée de la formation, des nombreuses possibilités et de l'évolution démographique, il faudra du temps avant que les mesures appropriées ne prennent effet. Le problème du manque de travailleurs qualifiés qui accable les entreprises n'est donc pas prêt de disparaître dans les années à venir. Sans le soutien d'une équipe d'experts compétents en cybersécurité, capables de réagir rapidement en cas d'attaque, il est difficile pour les entreprises de se protéger contre des cybercriminels de plus en plus professionnels.

L'IA change les règles de la cybersécurité

Le concept d'intelligence artificielle peut sembler être une version de luxe de la sécurité informatique, surtout pour les petites et moyennes entreprises. Cependant, elle devient de plus en plus une technologie de base indispensable, d'autant plus que les cybercriminels l'utilisent déjà pour développer des logiciels malveillants intelligents. L'IA leur permet de modifier automatiquement les modèles d'at-

L'EXPERTISE DELL TECHNOLOGIES

Trois domaines sont essentiels à la sécurité informatique : une infrastructure sécurisée (terminaux, réseau et données), un protocole de sécurité avancé (réaction automatique aux menaces) et une gestion complète des risques (évaluation de l'ensemble des risques pour l'entreprise). Dell Technologies fournit aux entreprises des solutions et des services adaptés quel que soit le domaine, qu'il s'agisse d'appareils, d'applications d'un centre de données ou de services de cloud computing. Ainsi, les entreprises de taille moyenne qui ne disposent pas de ressources informatiques importantes peuvent se focaliser sur leur cœur de métier et faire confiance à DELL Technologies et leurs partenaires.



taque et de les camoufler au-delà de toute reconnaissance. Les fabricants n'ont alors d'autres choix que d'utiliser eux-mêmes l'IA s'ils souhaitent pouvoir se défendre.

Son utilisation dans les solutions de cybersécurité est vouée à se normaliser dans les années à venir. L'IA est un domaine d'application idéal en raison de sa capacité à analyser d'énormes volumes de données et donc à apprendre des modèles de comportement. Même si les solutions actuelles peuvent être décrites comme des solutions de sécurité IA de « première génération », qui visent principalement à rechercher des bases de données, à traquer les menaces et à faciliter la résolution des incidents de sécurité, à l'avenir, l'IA pourrait être utilisée pour automatiser les SOC (*Security Operations Centers*) fonctionnant 24 heures sur 24. Le personnel informatique disposerait ainsi de plus de temps pour les tâches stratégiques.

Si vous avez le regard tourné vers l'avenir, à un moment donné, même les ordinateurs quantiques changeront la donne en matière de cybersécurité. Ces superordinateurs résolvent à merveille des tâches complexes et ce de façon extrêmement rapide, car ils ne fonctionnent pas avec les valeurs 0 et 1 comme les ordinateurs classiques, mais peuvent calculer un grand nombre de gradations en une seule étape. Leur utilisation permettra d'accroître les performances des systèmes, des calculs et des transactions jusqu'à un niveau encore jamais atteint. Néanmoins, ces superordinateurs peuvent également devenir un atout pour les cybercriminels.

Cybersécurité : un combat sans fin

Aujourd'hui déjà, le secteur de la sécurité informatique, d'une part, et les pirates informatiques, d'autre part, sont engagés dans une course mutuelle à l'armement qui semble sans fin. Il est avéré que le thème de la sécurité informatique prend de plus en plus d'importance en raison du nombre croissant de cyberattaques qui utilisent des méthodes toujours plus sophistiquées. Par ailleurs, les moyennes entreprises devraient lui accorder une importance toute particulière. En effet, ces dernières se situent de plus en plus dans la ligne de mire des cybercriminels. Même si les précautions de sécurité en elles-mêmes ne créent pas de valeur ajoutée directe, elles permettent de prévenir les attaques qui menacent l'existence de l'entreprise. Si les ordinateurs tombent en panne et les machines s'arrêtent, les défaillances liées aux données peuvent engendrer des dépenses considérables. La mise en ligne de données sensibles sur la clientèle ou le simple accès à celles-ci par des tiers constituent un problème au moins aussi grave qui peut conduire à une perte de confiance.

INTEL® INTÈGRE DES FONCTIONS DE SÉCURITÉ DIRECTEMENT DANS LE COEUR

La protection des systèmes informatiques au moyen de logiciels de sécurité appropriés est renforcée efficacement par des fonctions de sécurité intégrées au matériel. La technologie Threat Detection Technology (TDT), fournie par Intel®, intègre ces fonctions directement au silicium afin de protéger chaque recoin de ces ordinateurs (matériel, firmware, système d'exploitation, applications, réseaux et cloud). A cette fin, la technologie Intel® TDT utilise une combinaison de données CPU, d'algorithmes lisibles par la machine et de graphiques intégrés pour les charges de travail liées à la sécurité et peut être incorporée aux solutions provenant de fournisseurs de logiciels indépendants afin d'étendre les fonctions déjà existantes. Cette technologie de détection des menaces est principalement destinée à faciliter la recherche de codes malveillants et est compatible avec les logiciels antivirus pour la recherche de logiciels et codes malveillants au sein du système.