INTELLIGENCE TI.
INTELLIGENCE
HUMAINE.

LES 6 FAILLES

DE SÉCURITÉ INFORMATIQUE LES PLUS COMMUNES

(ET COMMENT LES PRÉVENIR)

D’entrée de jeu, clarifions un point important : la sécurité en technologies de l’information ne sera jamais garantie à 100%.

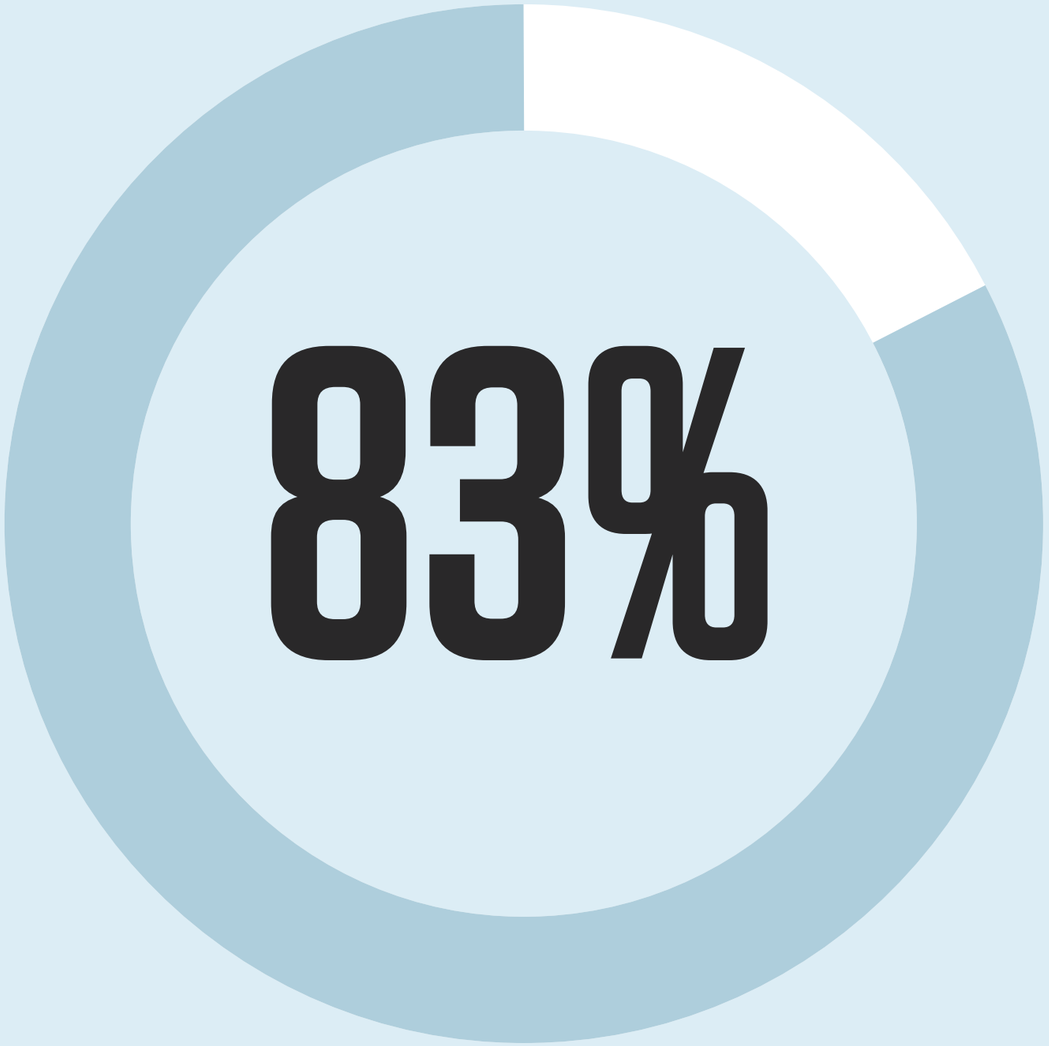
Plusieurs facteurs intrinsèques à l’informatique rendent cet objectif hors de portée. Les systèmes sont de plus en plus complexes et en évolution constante; deux éléments qui ajoutent un défi supplémentaire à la détection de vulnérabilités. Il ne faut pas non plus négliger le facteur humain, qui malgré les formations et la sensibilisation, demeure toujours une cause importante de brèches de sécurité.

SECTION 1

QU’EST-CE QU’UNE FAILLE?

Une faille est une faiblesse ou une vulnérabilité dans un système, une application, un réseau ou un processus qui peut être exploitée pour en compromettre la sécurité ou la stabilité. Il existe plusieurs familles de vulnérabilités, que nous avons réparties en fonction des caractéristiques qu'elles représentent.

Parmi les plus courantes, notons les vulnérabilités du réseau, du matériel ou des logiciels. Il y a aussi les failles causées par une mauvaise gestion des correctifs ou des erreurs de configurations. L'authentification des usagers, quant à elle, est une faiblesse très souvent exploitée par les cybercriminels. Et pour finir, l'ingénierie sociale exploite l'erreur humaine afin d'accéder à vos informations confidentielles.



Verizon relève que 83% des brèches proviennent de l’externe[1].

Que recherchent les pirates informatiques et pourquoi ?

Dans son rapport 2023 Data Breach Investigations Report[1], Verizon relève que 83 % des brèches proviennent de l'externe. Une fois sur deux, l'attaquant tente de s'approprier des informations d'identification. En d'autres mots, il recherche une façon « légitime » d'accéder au système pour s'y installer sans être détecté. On comprend rapidement pourquoi le facteur humain est impliqué dans 74 % des cas.

Les pirates informatiques ont diverses motivations pour vouloir accéder à des données d'entreprise, mais la principale pour plusieurs d'entre eux demeure financière. Ils cherchent à voler des données sensibles, telles que des informations de carte de crédit, des données bancaires, des informations de compte, des secrets d'entreprises ou des données personnelles qu'ils peuvent ensuite monnayer sur le marché noir. Ces données peuvent être utilisées pour commettre des fraudes financières, l'usurpation d'identité, le vol de fonds ou la demande de rançon aux propriétaires légitimes en échange de la restitution des données.

Certaines attaques informatiques visent à voler des informations sensibles liées à la propriété intellectuelle, aux secrets commerciaux ou à la recherche et développement. Les pirates, souvent mandatés par des concurrents ou certains États, cherchent à obtenir un avantage concurrentiel en accédant aux plans, aux prototypes, aux formules ou à d'autres informations confidentielles d'une entreprise.

Parfois, les pirates ont des motivations purement malveillantes, telles que la vengeance, la dissuasion ou l'extorsion. Ils peuvent chercher à saboter les opérations d'une entreprise en perturbant ses systèmes informatiques, en bloquant l'accès aux données critiques ou en divulguant des informations compromettantes. Les pirates peuvent ensuite demander une rançon en échange de la réparation des dommages ou de la non-divulgation des données volées.

Il est essentiel pour les entreprises de comprendre ces motivations pour mieux se prémunir contre les attaques et protéger leurs données sensibles. Cela implique la mise en place de mesures concertées et coordonnées de sécurité.

1 https://www.verizon.com/business/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001

Alors, comment s’en sortir ?

Comment les organisations peuvent-elles éviter des conséquences graves comme la perte de revenus, l’atteinte à la réputation ou à la vie privée ?

Il faut trouver l’équilibre entre sécurité et fonctionnalité en tenant compte de l’importance des actifs informationnels à protéger et des moyens financiers à votre disposition. Bref, c’est une question de gestion des risques.

Ce livre blanc aborde les failles et les vulnérabilités les plus communes selon nos équipes. Il est le résultat d’une rencontre très enrichissante où nos experts ont partagé différents cas de figure qu’ils rencontrent régulièrement dans leur pratique. Nous espérons que ce dossier vous apportera quelques éléments de réponses pour vous aider à faire face aux menaces.

Voici un survol des brèches les plus communes où, la plupart du temps, l’humain est impliqué, que ce soit de façon volontaire ou non intentionnel.

SECTION 2

LES 6 FAILLES DE SÉCURITÉ INFORMATIQUE LES PLUS COMMUNES

FAILLE #1

VULNÉRABILITÉS D'AUTHENTIFICATION

Le vol d’identité demeure un défi majeur, et les mots de passe traditionnels ne sont plus suffisants pour garantir la sécurité. Voici des mesures de protection à mettre en place sans plus attendre.

L’authentification multifacteurs (MFA)

Peu importe la méthode choisie, elle renforce considérablement la sécurité.

L’authentification unique (SSO)

Elle simplifie grandement la gestion des mots de passe et la sécurité en permettant une authentification unique pour accéder à différents systèmes ou applications.

Gestion des droits d’administrateurs

La limitation des droits d’administrateur est essentielle pour réduire les risques.

Principe d’accès minimal

Les utilisateurs ne doivent avoir accès qu’aux ressources nécessaires à leurs tâches.

Confiance nulle (Zéro Trust)

Adoptez cette approche qui a comme prémisse de faire confiance à rien ni à personne sans vérification et validation.

FAILLE #2

INGÉNIERIE SOCIALE

Les attaques d’ingénierie sociale, telles que l’hameçonnage et les rançongiciels, sont de plus en plus sophistiquées et se sont multipliées de façon exponentielle ces dernières années. Pour contrer ces menaces, les mesures sont simples, mais il faut y revenir souvent en raison du facteur humain qui est impliqué.

Sensibilisation des utilisateurs

La formation et la sensibilisation des usagers sont essentielles pour les garder vigilants contre les attaques d’ingénierie sociale.

Rappels réguliers

Les rappels périodiques et ludiques renforcent la sensibilisation des utilisateurs. Testez, mesurez, formez et recommencez.

Meilleure protection des courriels

D’un point de vue strictement technologique, utilisez des solutions de filtrage et de détection avancées pour réduire les attaques par hameçonnage.

FAILLE #3

VULNÉRABILITÉS DE SÉCURITÉ LOGICIELLE

Les vulnérabilités de sécurité logicielle sont des champs de bataille majeurs pour les attaquants. Les injections et les logiciels malveillants sont des menaces courantes, car chaque nouvelle version d'un logiciel entraine dans son sillage de nouvelles vulnérabilités exploitables. Pour contrer ces failles, voici quatre éléments importants.

Contrôle d'accès basé sur les rôles (RBAC)

Définissez des permissions précises pour les utilisateurs en fonction de leurs rôles.

Contrôle d'accès conditionnel

Limitez l'accès en fonction de la sensibilité des applications, de la localisation et des utilisateurs.

Groupe de gestion

Offrez de l'autonomie aux équipes et facilitez la gestion des permissions et des droits d'accès à des fichiers, des documents, des applications de façon collective plutôt qu'individuelle.

Maximiser l'activation des protections disponibles sous Microsoft

Utilisez les fonctionnalités d'Entra ID et Microsoft Defender pour identifier et gérer les applications non autorisées et pour limiter les actions qui pourraient compromettre la sécurité de l'environnement.

4

FAILLE #4

VULNÉRABILITÉS DES PÉRIPHÉRIQUES

Les vulnérabilités matérielles incluent les virus, les logiciels malveillants et les utilisateurs disposant de droits d'administrateur local. Pour réduire ces risques, il est essentiel de prendre les mesures suivantes.

→ Protection contre les virus et les logiciels malveillants

Ce moyen de protection est sûrement le plus connu et doit être utilisé en combinaison avec une solution EDR (Endpoint Detection and Response) pour détecter rapidement les menaces avancées et les activités suspectes et répondre plus efficacement aux incidents.

→ Limitation des droits d'administrateur local

Réduire au minimum ces droits pour limiter les capacités des utilisateurs à apporter des modifications majeures aux systèmes.

→ Chiffrement des disques locaux

L'utilisation de solutions telles que Bitlocker permet de protéger les données stockées localement.

→ Gestion centralisée des appareils

Même pour les appareils utilisés hors de votre périmètre sécurisé, l'utilisation d'outils comme Intune permet une gestion centralisée et la possibilité d'effacer à distance les appareils en cas de perte ou de vol. Intune permet également de gérer et sécuriser les appareils personnels des employés, dans un contexte professionnel, notamment en surveillant l'état de conformité des équipements afin de protéger les ressources de l'entreprise.

→ Renforcement de la sécurité des appareils (device hardening)

Sa démarche par étapes vise à rendre les dispositifs matériels moins susceptibles d'être compromis par des attaques malveillantes, par exemple en désactivant les fonctionnalités non essentielles ou en effectuant les mises à jour des logiciels.

5

FAILLE #5

VULNÉRABILITÉS DU RÉSEAU

Les vulnérabilités des réseaux sont des failles ou des erreurs dans la conception, la configuration ou la maintenance, qui peuvent être exploitées par des attaquants pour accéder aux données ou aux services.

Parmi les menaces auxquelles les réseaux sont confrontés, citons les tentatives de vol des identifiants qui demeurent l'une des plus courantes. Elles visent à subtiliser, par exemple, votre nom d'utilisateur et votre mot de passe dans le but de compromettre le compte visé. Pour se prémunir contre ces types de menaces liées, il est essentiel d'aller au-delà des classiques pare-feux.

Le rôle d’un centre opérationnel de sécurité (SOC)

Qu’il soit interne ou imparti, est de détecter, analyser, répondre et prévenir les incidents de sécurité.

Système de gestion des informations et des événements de sécurité (SIEM)

Ce système est l’outil principal du SOC. Il fournit une vue d’ensemble des événements, anomalies et menaces de sécurité en collectant et corrélant les données provenant de diverses sources.

Contrôle d’accès réseau (NAC)

Il gère et module les accès en fonction du type d’appareil connecté et de l’utilisateur selon des stratégies prédéfinies. Par exemple, un administrateur peut bénéficier d’un accès privilégié, tandis qu’une imprimante peut avoir un accès restreint.

L’approche de la Confiance nulle (Zero-Trust Network Access ou ZTNA)

Cette approche vérifie si un poste ou un utilisateur respecte les critères de conformité de l’entreprise avant de l’autoriser. Des solutions telles que FortiClient, Cisco DUO, ou Microsoft Intune permettent de définir un périmètre dynamique, basé sur l’identité numérique et d’appliquer des règles définies selon le contexte. Ces outils sont des compléments venant renforcer les solutions d’authentification et d’accès tel qu’Entra ID, par exemple.

Protection de contenu réseau

Essentielle pour les travailleurs à distance, notamment dans le cadre des architectures SASE (Secure Access Service Edge) et SSE (Secure Service Edge). Celles-ci visent à sécuriser les données et ressources accessibles via un réseau, garantissant ainsi la confidentialité et l’intégrité des informations, mais également que ces contenus soient eux-mêmes sécuritaires. Par exemple, on peut bloquer les pages web qui sont caractérisées comme étant non légitimées ou non autorisées.

Protection des appareils et des objets connectés (IOT) et sécurité des technologies opérationnelles (OT)

Les dispositifs utilisés dans les environnements industriels peuvent constituer des points faibles et il est crucial de garantir leur sécurité, notamment pas la segmentation réseau ou le contrôle d’accès, afin de garantir la continuité des opérations et la sécurité des processus critiques.

6

FAILLE #6

VULNÉRABILITÉS DANS LA GESTION DES CORRECTIFS ET DES CONFIGURATIONS

Les vulnérabilités liées à la gestion des correctifs et les erreurs de configuration sont autant de menaces. Pour atténuer ces risques, voici ce que nos experts recommandent.

Configuration judicieuse des services infonuagiques

Les solutions comme Azure ou Microsoft 365 offrent des avantages énormes, mais requiert une stratégie de sécurité réfléchie et avisée afin d'être configurées selon les meilleures pratiques de l'industrie.

Responsabilité partagée de la sécurité

Les fournisseurs de services infonuagiques partagent la responsabilité de la sécurité, mais sachez que vous avez aussi votre part. Pour chaque solution, vous devez connaître votre périmètre et le gérer.

Conscientisation des utilisateurs

La simplicité d'installation des logiciels peut conduire à des vulnérabilités. Les utilisateurs doivent être conscients des risques et c'est votre devoir de vous assurer que les configurations sont sécuritaires et que les correctifs s'appliquent automatiquement.

SECTION 3

VOTRE PLAN DE RELÈVE

200

Repérer un cybercriminel dans vos systèmes peut prendre jusqu'à 200 jours[1].

1 https://www.verizon.com/business/resources/reports/dbir/?CMP=OOH_SMB_OTH_22222_MC_20200501_NA_NM20200079_00001

Il n’est pas évident de savoir si votre entreprise a été la cible d’une attaque. Pour soupçonner l’indétectable, il faut être sensible au moindre signe que quelque chose sort de l’ordinaire. Cela peut être des sommes d’argent qui disparaissent mystérieusement du compte de banque, des mots de passe qui ne fonctionnent plus ou des documents qui deviennent soudainement inaccessibles. C’est alors que vous devez déployer votre gestion de crise.

Étape 1 – Planifiez

En cas de cyberattaque présumée, la mise en œuvre d’un plan est cruciale. Simulez votre gestion de crise en incluant la liste de risques classés en fonction de leurs impacts potentiels. Faites également l’inventaire des actifs, en ordre de criticité, afin d’être en mesure de prioriser en temps de crise. Identifiez les parties prenantes pouvant être potentiellement concernées et établissez des moyens de communication en tenant compte des aspects technologiques, opérationnels, financiers, réputationnels et humains.

Étape 2 – Intervenez

Évaluez les conséquences de ce qui s’est passé et élaborez des plans à court, moyen et long terme. Si la préparation était suffisante, exécutez le plan préalablement élaboré. Gérez la communication et prenez en charge l’incident pour contrôler le message et conserver la confiance des clients et employés.

Étape 3 – Relevez-vous

Réagissez rapidement pour minimiser les dommages et leurs impacts. Évaluez les perturbations, les dégâts aux systèmes, les impacts financiers et sur l’image de l’entreprise. Résolvez les problèmes, prévenez de futures erreurs humaines, et restez vigilant face aux risques de cyberattaque récurrents.

Être proactif, une question d'assurances.

Les compagnies d'assurances ont resserré leurs critères de qualification à la suite de la recrudescence des attaques informatiques et de la forte hausse des réclamations. Les renouvellements sont loin d'être automatiques et les entreprises doivent maintenant démontrer qu'elles maîtrisent les bonnes pratiques en matière de protection de l'information.

Plusieurs facteurs analysés par les compagnies d'assurance influencent votre « cyberrisque » et auront donc un effet sur vos primes d'assurance. Quel type de données conservez-vous et sont-elles sensibles ? Avez-vous en place des éléments dissuasifs aux cyberattaques, telles des protections techniques (mots de passe, antivirus, pare-feu) ou une surveillance (SIEM ou SOC) pour dissuader ou détecter les intrusions?

La sécurité informatique ne peut jamais être garantie à 100 % en raison de la nature complexe et évolutive des systèmes, ainsi que du facteur humain. C'est pourquoi la vigilance, la préparation et la réactivité sont des atouts essentiels qui doivent faire partie de votre quotidien pour la protection des données et des actifs. Pour faire face à cette réalité, une gestion des risques équilibrée est essentielle.

Il peut s'avérer difficile d'effectuer un choix éclairé sur la méthodologie à utiliser pour évaluer votre niveau de risque. Si vous ne savez pas par où commencer, les spécialistes d'ITI peuvent vous aider à établir un portrait de votre posture de sécurité pour vous permettre de prioriser vos actions.

INFORMEZ-VOUS SUR NOS OFFRES DE BILAN DE MATURITÉ EN SÉCURITÉ

Planifier une rencontre avec nos spécialistes →