Les six choses à faire pour éviter 95% des attaques informatiques

Les six choses à faire pour éviter 95% des attaques informatiques

La cybersécurité est essentielle, d'accord, mais par où commencer ? Pour vous aider à faire le premier pas, nous avons identifier 6 principes clés qui, lorsqu'ils sont suivis, peuvent éviter la grande majorité des attaques.

1/ FAIRE DE LA SÉCURITÉ UN PROCESS (CE N'EST PAS UN PRODUIT)

« Je dois protéger mon entreprise ? Certes. Quel produit faut-il que j'achète ? » La réflexion peut sembler naturelle. Après tout, autant faire appel à des professionnels. Le problème, c'est qu'on ne sécurise pas son entreprise en signant un chèque. La cybersécurité est avant tout une façon de penser, et passe par une organisation, par la mise en place de règles et méthodes. Elle implique de connaître son système d'information sur le bout des doigts pour en cartographier la surface d'attaque, de savoir tout ce qui est connecté (et ce qui ne doit pas l'être). Elle implique aussi de déterminer quels sont les services et les données qui sont réellement cruciaux au fonctionnement de la structure pour s'assurer que l'on concentre ses forces là où elles doivent l'être, sans s'évertuer à défendre plus que nécessaire des ressources non critiques. *« La sécurité est une composante au service du coeur de métier,* explique Eric Filiol, directeur du laboratoire de virologie et de #cryptologie opérationnelles de l'école d'ingénieurs ESIEA. *Il faut comprendre son métier et ce qui est critique. »* La stratégie doit être sensée pour que les ressources engagées (financières, humaines, temporelles) soient utilisées au mieux.

2/ PATCHER, PATCHER, PATCHER

Les révélations sur les méthodes de la NSA ou les gros titres sur les attaques contre des opérateurs d'importance vitale qui s'étalent sur des mois voire des années peuvent laisser penser que les hackers exploitent systématiquement des failles complexes et jamais référencées (appelées « zero days ») pour s'infiltrer dans un SI. Rien n'est moins vrai. Ces zero days ne sont utilisés qu'extrêmement rarement et seulement pour les cibles les plus importantes. La très grande majorité des attaques ciblent au contraire des failles bien connues et pour lesquelles existent déjà des correctifs de sécurité, souvent depuis des années. C'est pourquoi il est capital de faire systématiquement ces mises à jour (aussi bien pour le système d'exploitation que les frameworks ou les applications), et de concevoir son SI autour de cette nécessité. *« Il faut savoir que les criminels font du reserve engineering sur les patchs dès leur sortie pour exploiter les failles qu'ils corrigent. Auparavant cela leur prenait des mois, aujourd'hui ce ne sont plus que des heures,* détaille Thomas Tschersich, director of IT security chez Deutsche Telekom.*Et ils automatisent ensuite le processus pour toucher de très nombreuses cibles. »* Et ce besoin reste le même dans le cas d'un environnement de production industriel qui se doit d'être opérationnel 365 jours par an. La perception selon laquelle les environnements industriels sont fondamentalement différents des environnements de bureau est fausse et contribue à renforcer leur vulnérabilité.

3/ NE PAS SE CROIRE NON CONCERNÉ

Si les réseaux industriels sont de plus en plus visés par des attaques informatiques, c'est parce qu'ils y sont particulièrement vulnérables. La faute à l'évolution dramatique de la connectivité à Internet au cours des 20 dernières années. Lors de leur conception, il était assumé que ces systèmes ne couraient pas de risques car ils n'étaient pas visibles. Quand bien même ce fut jamais vrai, ce n'est définitivement plus le cas. Des services gratuits comme shodan.io permettent depuis des années de chercher parmi des centaines de milliers de systèmes ouverts, connectés à Internet sans aucune protection. Cela va de simples caméras de surveillance (résidentielles ou industrielles) jusqu'aux ICS qui supervisent le parc machine, que les opérateurs laissent sans protection car ils veulent pouvoir en prendre facilement le contrôle à distance. *« Il y a beaucoup de négligence et de mauvaises pratiques,* assène Frédéric Planchon, PDG de FPC Ingénierie. *Cela laisse des portes ouvertes à des malwares qui ne sont normalement pas si nocifs. »* Peu importe la taille de votre installation ou la nature de votre activité, si vous êtes vulnérables, vous serez tôt ou tard attaqué. Et ce même lorsqu'il n'y a rien à en obtenir, car de nombreux hackers agissent simplement « pour le sport ».

4/ PROTÉGER SES DONNÉES

La meilleure façon de garantir la sécurité de ses données, que ce soit contre le vol ou contre des attaques de type ransomwares, c'est de prendre les mesures adéquates en amont. Cela passe par deux axes clés : le chiffrement et la sauvegarde. Le chiffrement garantit que seuls les individus autorisés peuvent accéder aux données, même si le canal de communication ou le support de stockage est compromis. Ainsi, même en cas de vol, les dégâts restent minimaux. De son côté, la sauvegarde évite la perte de données, qu'elle soit dûe à un accident ou à un acte de malveillance. Une politique de sauvegarde rigoureuse et régulière peut faire la différence entre « plus de peur que de mal » et « la clé sous la porte ».

5/ FORMER SES TROUPES

Une vaste majorité d'attaques ont un point commun : l'erreur humaine. Un collaborateur qui ouvre le mauvais email ou clique sur le mauvais lien. Un autre qui perd son appareil ou sa clé USB. Un troisième qui laisse traîner ses identifiants de connexion (ex. post-it sur l'écran) ou les communique par erreur/inattention… La sécurité n'est pas innée, elle s'enseigne. Il est impératif de former les équipes aux bonnes pratiques à adopter et de les sensibiliser aux conséquences que la négligence peut avoir. Les rendre personnellement responsables de la protection de leurs données et appareils au travers de mesures simples peut suffire à largement diminuer les accidents.

6/ SÉCURISER AUSSI LES ACCÈS PHYSIQUES

Une #attaque informatique n'est pas forcément menée depuis l'autre bout du monde. Il faut donc s'assurer en premier lieu que le périmètre de l'entreprise est sécurisé pour limiter les accès non autorisés en interne. Car le « social engineering », qui consiste à obtenir accès à un système en trompant son interlocuteur, est au coeur de nombreuses attaques. Il suffit parfois de mettre un uniforme de réparateur, de prendre une boîte à outils et de demander poliment l'accès à un local technique pour qu'on vous ouvre. Ou de mettre un costume et de se tenir devant une porte les bras chargés de documents. *« Nous appelons ça les attaques 'femme de ménage', et cela permet de prendre le contrôle d'un serveur en 5 secondes, »* explique Eric Filiol. Autre exemple, lorsque le réseau Wi-Fi interne d'une usine, non protégé car l'accès au bâtiment est restreint, peut aussi être capté depuis le parking… Les cas de figure sont nombreux et leur exploitation bien documentée. Ces éléments doivent donc systématiquement être pris en compte.

Article de Julien BERGOUNHOUX

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet…) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Cybersécurité : Les six choses à faire pour éviter 95% des attaques*