Le hacker qui s'ignore

Si les salariés mal intentionnés sont les plus médiatisés, la vraie menace interne vient de négligences ou de simples erreurs d'inattention

Il fut un temps où la principale mission des équipes de sécurité informatique était d'ériger des remparts impénétrables autour des systèmes d'entreprise.

Empêcher les pirates de s'infiltrer et les données de fuiter. Colmater les brèches et renforcer la sécurité des systèmes, des utilisateurs et de la propriété intellectuelle est un éternel recommencement.

Mais aujourd'hui les professionnels de la sécurité sont confrontés à un nouveau problème : l'inquiétante augmentation des vulnérabilités au sein même de la forteresse.

Bien souvent, on a tendance à associer les menaces internes à des salariés malveillants qui volent des informations, manipulent des données ou sabotent des systèmes informatiques. Mais une autre menace fait tout autant de dégâts : la négligence et l'inattention.

Si les incidents de sécurité majeurs dont les médias se font l'écho incitent plus volontiers à la prudence, leur côté spectaculaire ne devrait pas faire oublier que la menace interne est elle aussi omniprésente. En fait, c'est son côté ordinaire, presque routinier, qui doit capter l'attention des RSSI. Pas très glamour, mais tout aussi dangereux que les menaces externes.

Le danger vient de l'intérieur

Piratages et attaques en tout genre ont beau monopoliser le débat de la sécurité informatique, ce sont les négligences des salariés et fournisseurs qui présentent en réalité le plus de danger. Dès lors qu'ils sont munis de droits d'accès aux systèmes et aux données, ces collaborateurs peuvent en effet causer encore plus de dégâts que les cybercriminels : perte de propriété intellectuelle, interruption des opérations, dégradation de la réputation, érosion de la confiance des clients, fuites de données sensibles à des tiers, dont la presse, etc.

Les entreprises commencent à prendre conscience du problème. Toutefois, selon une étude menée par l'institut SANS[1], elles sont encore un tiers à n'avoir aucun système en place pour détecter ou prévenir les attaques de l'intérieur.

39 %

SEULES 39 % DES ENTREPRISES DANS LE MONDE PENSENT QUE LEURS SALARIÉS COMPRENNENT LEUR POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Par ailleurs, d'après le rapport Risk:Value de NTT en 2018[2], parmi les 57 % d'entreprises disposant d'une politique de sécurité de l'information, 81 % en ont informé leurs salariés, mais seulement 39 % estiment que ceux-ci en comprennent la teneur. Voilà qui devrait finir de convaincre celles et ceux qui douteraient encore de l'ampleur de la menace. À en croire les demandes adressées au comité britannique pour la protection des données (ICO) dans le cadre de la disposition *Freedom of Information*, les erreurs des salariés sont à l'origine de près de la moitié des incidents de sécurité subis ces dernières années.

L'émergence des réseaux *zero-trust* témoigne de la prise de conscience de certaines entreprises vis-à-vis des menaces internes. Comme son nom l'indique, cette approche considère qu'il n'y a plus de « zone de confiance » dans la sécurité de l'information.

Cependant, le *zero-trust* reste un concept souvent difficile à mettre en pratique, étant donné qu'un minimum de confiance doit tout de même être accordé aux salariés. Il existe donc un risque d'incompatibilité avec la philosophie de l'entreprise, son image de marque ou encore l'évolution de sa transformation numérique.

Les différents types de menaces internes

Si les collaborateurs internes représentent une menace à divers égards, on peut cependant classer la plupart dans trois grandes catégories :

1. Menace interne accidentelle

Tout le monde fait des erreurs. Même le plus loyal de vos salariés. Envoyer accidentellement le compte de résultat de l'entreprise à un concurrent est une erreur vite arrivée. Il suffit que le remplissage automatique des adresses e-mail soit activé et que plusieurs de vos contacts Outlook aient le même prénom. Des accidents, il y en aura toujours. Reste à savoir comment votre entreprise réagira et quelles mesures seront prises pour en réduire la probabilité.

2. Menace interne par négligence

Par souci d'efficacité, certains salariés contournent parfois les protocoles de sécurité mis en place par l'équipe IT.

Une imprudence qui peut s'avérer fatale. Nous recevons tous ces alertes nous demandant d'installer des correctifs de sécurité ou de mettre à jour un logiciel ou un navigateur. Mais combien d'entre nous y font vraiment attention ? Et combien n'hésiteraient pas à installer des logiciels non autorisés pour gagner en efficacité ?

3. Menace interne malveillante

Il est difficile pour une entreprise de protéger ses données contre un collaborateur interne déterminé et mal intentionné. Les cas d'exfiltration de données confidentielles au profit d'un nouvel employeur sont d'ailleurs en hausse. Plus le poste est élevé dans la hiérarchie, plus les droits d'accès aux données sensibles sont étendus, et plus les dégâts peuvent être considérables.

Par ailleurs, on assiste à un nouveau phénomène d'**alliance malveillante** entre salariés et acteurs externes. Selon des chercheurs en Threat Intelligence du cabinet IntSights[3], les hackers cherchent désormais à recruter des salariés dans le cadre d'opérations de délits d'initiés ou de vol en masse de numéros de cartes de paiement.

Si cette nouvelle pratique n'a rien de rassurant, la négligence et les erreurs n'en demeurent pas moins les menaces internes les plus répandues. Depuis début 2016, seul un quart des interventions de NTT Security sur des incidents internes était le fruit d'un acte manifestement hostile. La plupart étaient de nature accidentelle ou résultaient d'une simple négligence.

Pour en savoir plus sur les types de menaces internes les plus répandus et les différentes techniques de gestion des risques, consultez le rapport semestriel du Global Threat Intelligence Center (GTIC) de NTT Security, Q3 2017.

Sensibiliser les salariés aux menaces internes

Au vu du danger que peut représenter la moindre négligence, il est impératif d'engager des actions de pédagogie auprès de tous les acteurs de votre entreprise. Concrètement, instaurez des mesures de sécurité à suivre et des comportements à adopter systématiquement, même quand personne n'est là pour surveiller.

Selon le rapport de NTT Security sur l'état des menaces dans le monde (GTIR), le phishing figure parmi les méthodes de prédilection des hackers pour faire main basse sur des données, ce qui révèle un manque de sensibilisation à la sécurité en interne.

Pour une acculturation de toutes les forces vives, les dirigeants doivent montrer la voie et les RH s'impliquer en permanence. Cette approche top-down permet de souligner l'importance de la sécurité pour la pérennité de l'entreprise. De leur côté, les RH doivent intégrer la sécurité au cœur de leurs processus de recrutement, de formation et de développement professionnel.

« Les RH ont un vrai rôle à jouer pour promouvoir une culture de la sécurité [...] en s'assurant de l'adhésion de tous les salariés à ces pratiques, en les incitant à la prudence dans leur quête de performances et en les responsabilisant pour qu'ils adoptent les bons réflexes et les inculquent à leurs collègues. »

– Heather Scallan, Vice-présidente senior des Ressources humaines chez NTT Security

Selon Heather Scallan, Vice-présidente senior des Ressources humaines chez NTT Security, « les RH ont un vrai rôle à jouer pour promouvoir une culture de la sécurité autour des valeurs fondamentales que sont l'intégrité, la diversité et la collaboration.

Pour ce faire, nous nous assurons de l'adhésion de tous les salariés à ces pratiques, nous les incitons à la prudence dans leur quête de performances et nous les responsabilisons pour qu'ils adoptent les bons réflexes et les inculquent à leurs collègues. »

Bien entendu, ces échanges entre collègues n'ont de sens que s'ils sont constructifs et bienveillants. Il faut donc veiller à guider et accompagner plutôt qu'à fliquer ou prendre de haut.

Certains attaquants vont jusqu'à cibler les dirigeants eux-mêmes dans leurs tentatives d'ingénierie sociale. Ils essaient ainsi de gagner leur confiance pour obtenir des codes d'accès ou autres informations confidentielles. Les bilans de vulnérabilités humaines menés par NTT Security pour ses clients révèlent que les cadres dirigeants peuvent compromettre la sécurité de leur entreprise en dix minutes seulement.

Les départements RH doivent se rapprocher des RSSI et autres dirigeants pour que chacun donne l'exemple. D'autres missions consisteront à mettre en place des formations sur-mesure et à identifier les menaces internes propres à chaque poste pour mieux préparer les équipes à se défendre.

Pour Heather Scallan, « faire équipe avec le RSSI nous permet de trouver plus facilement le bon équilibre entre la formation et la création d'une culture où chacun adopte la bonne attitude face aux risques de sécurité. »

Voir pour prévoir

Pour démasquer une menace interne, les entreprises doivent impérativement avoir une visibilité totale sur les indicateurs de risque de leur réseau. Si les pare-feu montent la garde aux points d'entrée, la visibilité est une sentinelle censée patrouiller pour détecter les anomalies. Registres d'accès, trafic réseau interne et infractions aux politiques sont autant de foyers d'activités suspectes qu'il faut surveiller.

Commencez par bien comprendre à quoi ressemble votre réseau au cours d'une journée type. Certaines personnes sont-elles habilitées à accéder à des données sensibles dans le cadre de leurs missions au quotidien ? Savez-vous précisément quelles sont les applications utilisées pour effectuer des opérations de base ?

Tout agissement anormal doit faire l'objet d'une enquête. Accès non-autorisé à un dossier ou un système, violation des politiques de sécurité, pertes ou mouvements suspects de gros volumes de données... tous ces indicateurs doivent être visibles pour vous permettre d'identifier des comportements singuliers.

L'importance d'une évaluation fiable des risques

Pour gérer efficacement toutes les typologies de menaces internes, vous devez connaître le degré de vulnérabilité de votre entreprise. En procédant à un bilan complet des risques et vulnérabilités, vous connaîtrez votre degré de préparation à la prévention, la détection et la neutralisation des menaces.

Ce bilan consiste, dans un premier temps, à identifier et localiser les données, la propriété intellectuelle et les systèmes vitaux pour l'entreprise. Cette étape, qui peut être intégrée à n'importe quel outil de détection, permet aux entreprises d'adopter une réponse à incident plus mature et mieux adaptée à leurs risques.

Ensuite, le bilan identifie les vulnérabilités techniques, les failles des processus et les problèmes de management, puis note l'entreprise sur sa capacité à détecter les comportements humains symptomatiques d'une menace imminente ou en cours.

D'expérience, nous savons que les menaces internes sont complexes. C'est pourquoi il vous faut opter pour une méthodologie d'évaluation qui englobe à la fois les personnes, les politiques, les pratiques et les technologies.

Services et solution à envisager

Pour surveiller le comportement des utilisateurs, on fait généralement appel à AD (Active Directory), aux journaux d'utilisateurs et aux proxys web. Cependant, ces pratiques-là ne permettent pas de détecter à temps les erreurs et autres entorses aux politiques en place qui sont le lot quotidien des entreprises. Or, ces comportements ouvrent un nombre incalculable de brèches.

Outre l'acculturation de votre entreprise aux pratiques de sécurité, des outils avancés tels que l'EDR (*Endpoint Detection and Response*) et l'UEBA (*User Entity and Behavior Analytics*) vous seront nécessaires pour détecter les menaces internes.

Mais avec des budgets et des ressources contraints, encore faudra-t-il savoir investir dans le bon mix de compétences, de procédés et de technologies. Par ailleurs, la création d'une culture de la sécurité peut exiger des compétences rarement présentes en interne.

Une option s'offre cependant à vous : opter pour un service de sécurité managé qui réduit les délais entre détection et neutralisation, tout en alliant Threat Intelligence contextualisée et analytique avancée pour améliorer la précision des interventions. Le machine learning, la modélisation des comportements et autres techniques de détection d'anomalies ont également un rôle à jouer dans la détection des menaces internes.

En cas de compromission avérée, il est primordial de pouvoir compter sur des procédures de réponse à incident bien définies, bien coordonnées et bien huilées pour neutraliser rapidement la menace, qu'elle soit externe ou interne. Malheureusement, le rapport Risk:Value de 2018 de NTT Security révèle que seule la moitié des entreprises sondées (57 %) dispose d'un plan de réponse à incident.

Face à ce chiffre inquiétant, vous aurez probablement tout intérêt à faire appel à un prestataire de services de sécurité managés (MSSP) qui apportera avec lui toute son expérience d'autres marchés et environnements technologiques.

Conclusion

Quand on entend « menaces internes », on pense tout de suite à Julian Assange, Edward Snowden et autres lanceurs d'alertes n'hésitant pas à divulguer des données hautement confidentielles pour des raisons idéologiques ou personnelles. Cependant, si une menace à la WikiLeaks reste tout à fait envisageable, les entreprises qui se concentrent essentiellement sur les attaques malveillantes risquent de se découvrir dangereusement sur un autre front, celui des négligences et des erreurs accidentelles. C'est pour cette raison que les RSSI ont tout intérêt à s'atteler à cette nouvelle priorité, et le plus tôt sera le mieux.

L'entreprise NTT Security

NTT Security est la branche et centre d'excellence sécurité du groupe NTT. Nous mettons notre expertise au service des entités du groupe NTT en délivrant des solutions métiers résilientes pour accompagner leurs clients dans leur transformation numérique. Forte de ses 10 centres opérationnels de sécurité (SOC), ses 7 centres de R&D et plus de 1 500 experts en sécurité, NTT Security intervient chaque année sur des centaines de milliers d'incidents à travers six continents.

Pour optimiser l'utilisation de nos ressources locales et libérer le potentiel de nos capacités mondiales, nous offrons un ensemble adapté de services de sécurité managés (MSS) mais également de conseil stratégique ou technologique aux entreprises. NTT Security fait partie intégrante du groupe NTT (Nippon Telegraph and Telephone Corporation), l'une des plus grandes entreprises de TIC au monde. Visitez **www.nttsecurity.com/fr-fr** pour en savoir plus sur NTT Security ou **www.ntt.co.jp/index_e.html** pour le groupe NTT.

1. SANS Institute : Insider Threats and the Need for Fast and Directed Response – 2015 *2. Rapport Risque-Valeur 2018, NTT Security*
3. IntSights 2017 : Monetizing the Insider: The Growing Symbiosis of Insiders and the Dark Web.