La convergence des systèmes de sécurité : nécessaire maintenant plus que jamais

Aujourd'hui, les projecteurs sont de plus en plus braqués sur la sécurité informatique, et le sujet alimente d'innombrables discussions dans le monde entier. La sécurité informatique s'est même invitée à l'ordre du jour au sommet de Genève de 2021, à la demande du président américain Joe Biden et du président russe Vladimir Poutine. Ces inquiétudes généralisées sont légitimes : le nombre d'attaques par ransomware a augmenté de près de 150 % en mars de l'année dernière, et de 102% au premier semestre 2021.

Les défaillances en matière de sécurité informatique entraînent des conséquences de plus en plus graves pour le monde physique, où les infrastructures essentielles et des vies humaines peuvent être mises en danger. Il suffit de prendre pour exemple le piratage d'une station d'épuration en Floride en 2021. Une faille dans le réseau informatique s'est rapidement transformée en un danger bien réel, menaçant d'empoisonner l'eau de toute une ville avec de dangereuses concentrations de soude.

Malgré cela, de nombreuses organisations continuent de faire fonctionner leurs équipes de sécurité physique et informatique comme des disciplines distinctes et autonomes, avec peu voire aucune collaboration entre elles en matière de gestion des risques.

Alors quelle est la solution ? Face à des menaces à la fois physiques et informatiques de plus en plus présentes, permettre à toutes les équipes de sécurité de collaborer efficacement est désormais un impératif stratégique pour les entreprises. Selon l'Agence américaine de cybersécurité et de sécurité des infrastructures (CISA), les fonctions de sécurité physique et informatique peuvent ainsi être plus résilientes et mieux préparées à identifier, prévenir, réduire et faire face aux menaces.

Comment en est-on arrivé là ?

Traditionnellement, les entreprises ont toujours séparé leurs opérations de sécurité physique et informatique. Cette différence s'explique par la différence d'ancienneté de chaque discipline : la sécurité physique existe depuis bien plus longtemps que la sécurité informatique, qui elle est plus récente.

Dataminr

Mais grâce à l'utilisation accrue des appareils IoT et IIoT, et face au nombre croissant de systèmes passant au cloud, de la prolifération des réseaux sociaux et des appareils connectés, la nécessité d'une convergence de la sécurité est plus grande que jamais.

Certains exemples de risques à la fois physiques et informatiques sont plus évidents, comme l'attaque par ransomware sur le système du système de santé irlandais en mai 2021. Celle-ci a interrompu l'ensemble du système informatique, devenant aussitôt une réelle menace pour des millions de patients. Ce fut aussi le cas de l'attaque contre la station d'épuration de Floride, précédemment citée.

Il existe de nombreux autre exemples qui, même s'ils ne sont pas aussi évidents, présentent des risques tout aussi importants. On pourrait citer l'augmentation récente du nombre d'attaques sur les systèmes de contrôle industriels (ICS) connectés à Internet, notamment ceux qui gèrent les infrastructures critiques du traitement des eaux et des usines de gaz, en passant par la circulation des trains et les systèmes de feux de signalisation. Dans certains cas, les hackers exploitent les failles de sécurité dans les contrôles d'accès aux installations, ce qui leur permet d'installer des logiciels malveillants et de compromettre ensuite l'ensemble du réseau d'une entreprise ou d'une organisation. Les logiciels d'accès à distance utilisés pour contrôler les ICS et les systèmes de chauffage, de ventilation et de climatisation sont également des points d'entrée courants pour des attaques qui touchent à la fois les domaines informatique et physique.

Pour un meilleur contrôle des menaces convergentes

Des organisations et entreprises pionnières associent de plus en plus leurs équipes de sécurité informatique et physique pour améliorer leur dispositif de sécurité global. Toutefois, cette fusion des deux services ne représente pas encore le modèle prédominant pour les opérations de sécurité.

Les experts affirment pourtant que le cloisonnement des équipes expose les entreprises à des défaillances opérationnelles et à un affaiblissement du niveau de sécurité. Par exemple, dès qu'une nouvelle menace apparaît, il arrive souvent que les responsables de la sécurité se concentrent uniquement sur leur domaine de responsabilité, sans savoir ce qui se passe ailleurs. Cette mauvaise habitude empêche les équipes de sécurité physique et informatique de disposer d'une vision globale des menaces potentielles.

Conjuguer l'expertise des responsables et des équipes en charge de la sécurité physique et informatique peut s'avérer difficile. Il existe souvent un fossé culturel et professionnel entre les deux, ce qui les amène à envisager les choses de manière radicalement différente. Ces différences peuvent se traduire par une mauvaise communication et parfois même par de graves incompréhensions, deux des plus gros problèmes auxquels sont confrontées les entreprises et les organisations qui n'ont pas encore développé de procédures solides pour favoriser la collaboration entre ces deux équipes essentielles.

Il faut également tenir compte des obstacles logistiques ainsi que du manque de compréhension de la direction quant à la raison pour laquelle la convergence de la sécurité n'est plus simplement une possibilité intéressante, mais un véritable impératif commercial.

Quand les équipes de sécurité unissent leurs forces

Les avantages d'un partenariat étroit entre les équipes chargées de la sécurité physique et informatique sont nombreux. Voici quelques exemples :

- Un dispositif de sécurité plus fort et plus global
- Une identification, une évaluation et une réponse plus rapides aux menaces informatiques et physiques
- Une meilleure communication et un meilleur partage des informations et des technologies
- Une amélioration de l'efficacité et des résultats

Chaque entreprise ou organisation gérera et réagira différemment à la convergence croissante des risques physiques et informatiques, mais c'est sur les informations en temps réel que reposera leur capacité à le faire. Elles doivent s'assurer que toutes les équipes de sécurité ont accès aux même données en temps réel sur les risques potentiels, indépendamment de l'endroit ou de la façon dont ils émergent. Elles doivent également créer des procédures claires pour savoir quand, à qui et comment communiquer ces informations.

Il est essentiel de pouvoir identifier ces événements et risques physiques et informatiques le plus tôt possible, et au fur et à mesure qu'ils se produisent et se déroulent. C'est pourquoi les entreprises qui travaillent avec Dataminr s'appuient sur Dataminr Pulse pour détecter les premiers signaux de risques émergents et d'événements pouvant entraîner d'importantes répercussions.

Lorsque le système d'oléoduc américain Colonial Pipeline a été frappé par une attaque de ransomware en mai 2021, Dataminr Pulse a alerté nos clients des problèmes de réseau qu'ils pourraient rencontrer un jour avant la diffusion de l'information par les médias. Dataminr Pulse a ensuite continué de les informer tout au long de l'évènement en fournissant le contexte nécessaire pour qu'ils puissent prendre toutes leurs décisions en parfaite connaissance de cause.

À mesure que la technologie progresse et s'intègre dans nos modes de vie et de travail, nous pouvons malheureusement nous attendre à une augmentation exponentielle des attaques physiques et informatiques comme celle ayant frappé Colonial Pipeline. Pour anticiper et réduire efficacement ces risques, les responsables de la sécurité, quels que soient leur domaine d'expertise ou leurs priorités, doivent s'assurer que leurs équipes travaillent en étroite collaboration pour contrer les menaces et partager à la fois les informations, les outils, les compétences et les ressources.

Pour en savoir plus sur l'intérêt des alertes en temps réel Dataminr Pulse , regardez ce webinaire à la demande et découvrez en quoi faire converger sécurité physique et informatique est aujourd'hui une nécessité.

Al Bowman est responsable des comptes d'entreprise chez Dataminr. Avant de rejoindre Dataminr, il a conçu, développé et dirigé le Centre de services de renseignement de Deloitte à Londres. Avant cela, il a servi dans l'armée britannique, où son dernier poste a été celui de directeur du centre mondial des risques et du renseignement de l'armée.

Dataminr