Cybersécurité & immobilier commercial

– Démystifier les tendances et menaces cyber

BOMA Québec
Symposium – Adaptation aux nouvelles réalités dans l'immobilier commercial
Novembre 2024

PSP

Geneviève Bertrand

Première directrice
Sécurité de l’information & gestion de crise
Investissements PSP

Introduction

La cybersécurité est un enjeu majeur pour les entreprises de toutes tailles et de toutes industries en raison de la sophistication croissante des cyberattaques et de l'importance des pertes financières, réputationnelles et opérationnelles potentielles.

- Menaces et tendances en cybersécurité
- Cybersécurité et immobilier commercial

Menaces et tendances en cybersécurité

Attaques par rançongiciel

Les attaques par rançongiciel sont une menace croissante, où les cybercriminels utilisent des logiciels malveillants pour bloquer l'accès aux données et demandent une rançon pour les restituer.

Attaques par hameçonnage

Les attaques par hameçonnage sont une méthode courante d'attaque, qui utilisent le courriel pour inciter les utilisateurs à divulguer des informations personnelles ou cliquer sur des liens malveillants.

Utilisation de l'intelligence artificielle dans la cybersécurité

L'utilisation de l'intelligence artificielle en cybersécurité est une tendance croissante. Les entreprises utilisent des systèmes d'IA pour détecter les menaces et renforcer la sécurité de leurs données, mais les acteurs malveillants font de même pour faciliter et augmenter la sophistication des cyberattaques.

Attaques par rançongiciel

Les attaques par rançongiciel sont une menace croissante pour les entreprises. Les cybercriminels cryptent les données de l'entreprise et demandent une rançon pour les débloquer.

Les attaques de rançongiciels peuvent causer des pertes financières considérables, avoir des conséquences opérationnelles significatives et engendrer un impact négatif sur la réputation de l'entreprise.

saviez-vous que ?

Le ransomware-as-a-service (RaaS) est un modèle commercial dans lequel des développeurs de rançongiciels louent leurs logiciels malveillants à d'autres cybercriminels, ce qui permet à des individus sans compétences techniques de mener des attaques.

Ce modèle a considérablement augmenté la fréquence et la sophistication des attaques de ransomware, rendant les entreprises de toutes tailles vulnérables.

Attaques par hameçonnage

L’hameçonnage et le piratage psychologique sont utilisés par les cybercriminels pour obtenir des informations personnelles, telles que des mots de passe ou des informations de carte de crédit, ou pour installer des logiciels malicieux.

Les attaques d’hameçonnage peuvent se manifester sous forme de courriels, SMS et messages vocaux. D’autres fraudes de type piratage psychologique arrivent par les médias sociaux et les sites web malveillants.

saviez-vous que ?

L’hameçonnage est la technique d’attaque la plus fructueuse utilisée par les cybercriminels. Jusqu’à 95% des cyberattaques réussies viennent de l’hameçonnage.

Parmi les cas d’usage les plus fructueux, des groupes de cybercriminels se font passer pour des employés du service d'assistance informatique et utilisent abusivement des outils de connexion à distance pour mener des attaques.

Intelligence artificielle

L'IA peut être utilisée pour détecter et prévenir les cyberattaques en temps réel…

L'IA peut analyser les données de sécurité pour identifier les tendances et aider les entreprises à comprendre les points faibles de leur système de sécurité et à renforcer leur cybersécurité…

… Mais l'IA a aussi ses limites et ses vulnérabilités, qu'il importe de bien comprendre pour éviter les erreurs coûteuses et les failles de sécurité.

saviez-vous que?

L'IA peut présenter différents types de risques en cybersécurité:

- en conduisant potentiellement à de la désinformation ou de la mésinformation;
- en permettant aux cybercriminels de créer des attaques par hameçonnage plus fréquentes, automatisées et sophistiquées; et
- en exposant des données sensibles qui auraient été fournies accidentellement par les utilisateurs dans leurs requêtes.

Cybersécurité et immobilier commercial

Violation des données

La violation des données implique l'accès non autorisé, la divulgation ou la destruction de données sensibles. Ces données incluent des informations personnelles sur les locataires, les propriétaires, les tiers, ainsi que des détails financiers et contractuels.

Les conséquences de telles violations peuvent être graves: pertes financières, dommages réputationnels, sanctions légales, etc.

Sécurité physique et IoT

La sécurité physique est un enjeu important dans l'immobilier commercial. Les entreprises doivent protéger leurs systèmes et équipements contre les intrusions, et mettre en place des mesures de sécurité pour les visiteurs et le personnel.

Parallèlement, les systèmes de gestion des bâtiments modernes intègrent de plus en plus de technologies basées sur l'Internet des objets (IoT), ce qui augmente la surface d'attaque potentielle.

Fraude de paiement

La fraude de paiement est une menace courante dans le secteur de l'immobilier commercial, que ce soit via la falsification de paiements, le piratage de comptes de paiements, et la manipulation frauduleuse de factures, entre autres.

Les vecteurs d’attaques sont aussi nombreux, mais l’un des plus fréquents est l’hameçonnage.

Risque de tiers

Les chaînes d'approvisionnement dans le secteur de l’immobilier commercial sont souvent complexes et impliquent de nombreux intervenants, ce qui augmente la vulnérabilité aux cyberattaques via les tiers.

- Vulnérabilités techniques
- Mises à jour de logiciels tiers
- Ingénierie sociale
- Vol d’identifiants de connexion

Risque de concentration

Petit frère du risque de tiers, le risque de concentration réfère à l'utilisation par de nombreux gestionnaires immobiliers et de bâtiments des mêmes quelques solutions technologiques pour gérer leur parc.

Si l'une de ces solutions est attaquée, l'impact sur le secteur au complet peut être considérable.

Et quand c’est un peu tout ça à la fois?...

LE CAS TARGET

En 2013, des cybercriminels ont infiltré Target via un **fournisseur tier** de systèmes **HVAC**. Une attaque par **hameçonnage** visant un employé de ce fournisseur leur a permis de voler des **identifiants de connexion** et d’accéder au réseau de Target. Les cybercriminels ont ensuite réussi à installer un **logiciel malveillant** sur les systèmes de point de vente de Target, **volant les informations** de plus de 70 millions de clients.

Aspect réglementaire en cybersécurité

Le secteur de l'immobilier au Québec et au Canada est soumis à plusieurs réglementations en matière de cybersécurité et de protection des données.

Loi 25 sur la protection des renseignements personnels des citoyens du Québec

Loi sur la protection des renseignements personnels et les documents électroniques

(LPRPDE/PIPEDA)

Règlement général sur la protection des données

(RGPD/GDPR)

Conclusion

Le secteur de l'immobilier commercial est confronté à plusieurs risques de cybersécurité, et la complexité des opérations immobilières rend ce secteur particulièrement vulnérable aux cyberattaques, dont la sophistication et la prévalence ne cessent de croître.

Les organisations doivent être conscientes de ces risques et mettre en place des mesures solides pour protéger leurs données et leurs systèmes.


Questions