COMMENT ABORDER LES TESTS D'INTRUSION

AVEC LA RÉALITÉ DES RANÇONGICIELS

En 2024, les entreprises tirent profit des technologies et doivent s'assurer de garder la confiance de leurs clients ainsi que de protéger les données de ces derniers.

Toutefois, les attaques par rançongiciels « ransomwares » ont augmenté de façon significative ces dernières années avec l'accroissement du travail à distance, l'utilisation grandissant des technologies et le nombre d'outils disponibles pour faciliter le travail des pirates. La raison est fort simple, le montant des rançons demandées est très élevé et plusieurs entreprises touchées sans les protections adéquates décident de payer (il est fortement déconseillé de céder aux menaces). Lors du paiement d'une rançon, les pirates promettent de rétablir les opérations, redonner l'accès à un environnement et aux données ainsi de ne pas diffuser les données confidentielles sur le web caché (darkweb).

Plusieurs facteurs expliquent pourquoi les rançongiciels arrivent à neutraliser les technologies utilisées par les entreprises :

- Les employés sont victimes d'hameçonnage pour obtenir des informations ou infiltrer une entreprise
- Les protections de sécurité TI sont absentes, inadéquates et les mesures de relève inefficaces
- Des vulnérabilités technologiques non corrigées
- Les nouvelles technologies sont en partie maîtrisées
- Les outils d'attaques sont de plus en plus puissants et faciles à utiliser
- L'utilisation de l'Intelligence artificielle améliore et diversifie les méthodes d'attaques
- Les outils d'attaque sont offerts en mode service SAAS aux pirates
- Des vulnérabilités présentes dans les applications
- Les technologies industrielles IOT sont également vulnérables
- Etc.

Tous ces facteurs doivent être contrôlés pour réduire les risques et les conséquences d'une attaque de rançongiciel.

Aucun secteur n'est maintenant à l'abri d'une attaque, ce n'est pas une question de la dimension de l'entreprise, mais plutôt de la valeur, des impacts et des conséquences qui amènent les pirates à identifier leurs cibles. Les entreprises au Québec ne font pas exceptions, les chiffres le démontrent et les publications d'incidents le confirment, aucune entreprise n'est à l'abri. Il faut également garder à l'esprit que plusieurs incidents ne sont pas identifiés ou restent confidentiels.

Tel que décrit dans plusieurs références, nombreuses technologies sont ciblées, plusieurs types d'attaques sont utilisés et plusieurs secteurs sont visés. Nous vous référons à des articles parus au cours des derniers mois :

- Canadian cyber threat intelligence annual report par PWC
- National cyber threat assessment by Canadian centrer for cybersecurity
- Crowdstrike 2024 global threat report
- Splunk Top 50 Cybersecurity Threats

Quoi faire

Il est fortement recommandé d'intégrer la protection de cybersécurité aux façons de faire, aux environnements technologiques et aux applications. Il est déconseillé de fonctionner en mode réactif, car l'impact et les conséquences d'une attaque seront encore plus importants, ainsi que le montant de la rançon.

Se dire que notre entreprise n'a aucun attrait pour des pirates est une erreur, toutes entreprises en opération qui utilisent des technologies et détiennent des données sont une cible potentielle. La seule différence peut être le type de pirates qui nous cibleront ou le montant de la rançon.
L'important est de prendre les mesures adéquates pour se protéger et de se préparer à réagir.

En 2024, il serait une erreur de fonctionner en mode réactif, car la survie d'une entreprise est dépendante de son environnement technologique, de ses données et de la confiance de ses clients.

Quelle approche choisir?

Pour identifier les failles d'un environnement technologique et les corriger, il est considérablement recommandé de procéder à des tests d'intrusion. Il existe deux approches, procéder à des tests d'intrusion standard ou avec un angle rançongiciel.

Approche standard

Les tests d'intrusion en général sont le processus de simulation des cyberattaques contre une organisation pour garantir que les contrôles de sécurité en place sont efficaces, découvrir et atténuer toutes les vulnérabilités résidant dans un environnement et fournir un récit d'attaque détaillé pour évaluer correctement la cyber résilience d'un environnement. Les activités de test de pénétration sont souvent classées par leur objectif dans les types suivants:

- Test de pénétration basée sur les objectifs
- Test de pénétration de l'infrastructure
- Test de sécurité des applications

Approche rançongiciel

Un test de pénétration rançongiciel comprend un test de pénétration complet ainsi que des composants d'évaluation technique et non technique qui évaluent le niveau de maturité de la cybersécurité d'une organisation, qui identifient les lacunes de sécurité chez les personnes, les processus et la technologie dans une organisation et qui testent la capacité d'une organisation à répondre

Test de pénétration complet: Une revue détaillée des configurations de réseau et de point de terminaison sur site, des configurations d'application infonuagique (cloud) et des mécanismes d'authentification et de chiffrement.

Évaluation des rançongiciels non techniques : Évalue les politiques administratives, les contrôles et la stratégie de risque d'une organisation et les compare aux meilleures pratiques standard de l'industrie pour déterminer le niveau de préparation à la cybersécurité d'une organisation et estimer sa

capacité à répondre et à se remettre d'une attaque de rançongiciel. Le résultat est une liste des observations et des recommandations pour prévenir les attaques de rançongiciels.

Ensemble, le test de pénétration complet, l'évaluation technique et l'évaluation non technique estiment l'impact potentiel du TTP connu, couramment utilisé par les acteurs des menaces de rançongiciel et fournir des informations qui peuvent être directement traduites en politiques et contrôles de sécurité améliorés.

Évitez de penser que l'absence de symptômes et de demandes de rançons signifie que vous n'êtes pas déjà la cible d'une attaque. Comme dans tous domaines, une attaque de rançongiciel se planifie et plus elle est bien orchestrée pour prendre le contrôle d'une grande portée, plus le montant de la rançon sera élevé.

SECURECOM peut vous guider pour déterminer l'approche qui convient le mieux à votre réalité et vous accompagner pour identifier et mettre en place les mesures qui vous conviennent.

Au cours des 20 dernières années, l'équipe aguerrie de SecurEcom, composée d'experts de haut calibre en TI, en gestion du risque en TI et en cybersécurité, a accompagné une clientèle reconnue au Québec, au Canada et aux États-Unis.

Des entreprises réputées, issues de divers secteurs dont les télécommunications, la finance, le transport, l'assurance, l'énergie, les technologies ainsi que de l'administration gouvernementale et publique ont eu recours aux services novateurs de SecurEcom dans leurs projets liés aux TI et à la cybersécurité et à la gestion du risque dans les TI.

N'hésitez pas à nous contacter : Alain Scherrer, associé principal

alain.scherrer@securecom.ca Tél. : 514 544-0442 poste 2320

Securecom.ca

Indik-dashboard.com