Threat Management

Un atout pour sécuriser vos essentiels

Au sein de l'écosystème actuel, les entreprises doivent adopter une approche globale pour se protéger contre la réalité des menaces avancées persistantes auxquelles elles peuvent être confrontées à l'avenir.

Les cyberattaques coûtent aux entreprises des millions de dollars en raison d'interruptions de service qui peuvent compromettre gravement leur intérêts ou e-réputation. The Ponemon Institute estime que le coût moyen d'une atteinte à la protection des données à l'échelle mondiale est désormais de 3,86 millions de dollars. En raison de l'évolution rapide de la menace, il est impossible, tant sur le plan économique que pratique, de dépêcher une sentinelle à chaque coin de rue. Une solution purement réactive construite autour des systèmes de défense traditionnels ne suffit plus pour écarter les acteurs malveillants. Une gestion globale des menaces peut aider à combler cette lacune. Elle propose une approche proactive à plusieurs niveaux, intégrant l'anticipation et la détection des menaces ainsi qu'une réponse rapide en cas d'incident.

Identifier les menaces qui pèsent sur leur activité

La gestion des menaces est conçue pour protéger contre toutes les cybermenaces, y compris celles croissantes que représentent les Advanced Persistent Threats (APT). Alors qu'elles n'étaient autrefois qu'un problème pour les cibles de premier plan telles que les gouvernements et les grandes multinationales, les APT représentent aujourd'hui une menace importante pour toutes les organisations.

Se préparer à l'imprévu

La question n'est plus tant de savoir si votre organisation sera attaquée, mais quand et comment elle le sera. Il est donc essentiel de mettre en place une stratégie de gestion des menaces mobilisant des experts capables de traiter les menaces connues. Cette expertise doit être associée à des processus éprouvés de détection, d'analyse et de remédiation, ainsi qu'à des outils de sécurité ayant fait leurs preuves.

196 jours en moyenne avant que les entreprises ne detectent une atteinte (1)

20% des domaines malveillants sont utilisés une semaine environ après enregistrement (2)

55% des alertes de sécurité provenant de logiciels antivirus sont des faux-positifs (3)

350% de croissance des attaques par rançongiciel chaque année (4)

1. Le coût caché des atteintes à la protection des données, Institut Ponemon, 2018
2. Rapport annuel de Cisco sur la cybersécurité, 2018
3. The Ponemon Institute State of Endpoint Security 2018
4. Rapport annuel de Cisco sur la cybersécurité, 2018

Orange
Cyberdefense

Minimiser le risque d'attaque

Les organisations doivent surmonter plusieurs défis importants en matière de gestion des menaces, en particulier lorsqu'il s'agit d'attaques avancées et coordonnées. Ces défis comprennent le manque de visibilité opérationnelle et de compétences internes pour surveiller et contenir les attaques sophistiquées ainsi que le trop grand nombre d'alertes que les équipes de sécurité doivent traiter.

Pour gérer au mieux les menaces, trois actions clés :

Détecter les menaces nouvelles et en mutation pour stopper ou limiter l'impact d'une brèche
La gestion et la qualification des alertes de sécurité nécessitent une technologie adéquate et des renseignements portant sur les menaces afin de réduire les faux-positifs, des experts capables de qualifier les alertes et de créer un plan d'action.

Réagir rapidement aux intrusions pour une intervention efficace en cas d'attaque
Cela comprend l'investigation sur l'incident et la remédiation ainsi que la possibilité de faire appel à des experts de notre équipe Investigation Numérique qui peuvent intervenir sur demande, au besoin, à distance et sur place.

Anticiper grâce à la Threat Intelligence
Pour protéger votre marque, il est nécessaire de surveiller en continu d'éventuels clonages malveillants de vos sites web ou applications, piratages des comptes des réseaux sociaux et d'identifier toute fuite de données sur le dark web par exemple.

Six étapes pour une gestion efficace des menaces

1. Effectuez une évaluation des risques
Il est nécessaire d'avoir une compéhension claire de la portée de vos actifs, notamment leur valeur et des règlementations sur lesquelles ils peuvent avoir une incidence, telles que le RGPD. Affectez votre budget de sécurité en fonction de la valeur de vos actifs, en particulier les données sensibles.

2. Adoptez une stratégie offensive d'anticipation
Les cybercriminels sont de plus en plus précis et focalisés sur les données. La Threat Intelligence vous aide à dessiner le profil de vos attaquants et de construire des scénarios portant sur la manière de contenir les attaques.

3. Effectuez un examen régulier de votre exposition face aux cybermenaces. Cela vous aidera à faire les ajustements nécessaires pour tirer le meilleur parti de vos capacités de detection, ainsi qu'à identifier les points d'entrée des plus récentes menaces, comme les logiciels malveillants sans fichiers (fileless malware).

4. Élaborez un plan complet de réponse à incidents
Il est essentiel que vous disposiez d'un plan d'intervention détaillé en cas d'incident qui soit propre à votre organisation et décrive les étapes de détection, d'enquête, de confinement, d'éradication et de rétablissement.

5. Partagez votre Threat Intelligence
Il est essentiel de suivre en permanence l'évolution de l'écosystème de la cybermenace pour prévenir les attaques. Si vous ne partagez votre connaissance de la menace pas vos propres renseignements, cela aura peu d'impact sur votre dispositif de sécurité.

6. Surveillez les menaces au-delà du périmètre de votre entreprise
La surveillance de l'internet visible, du dark et du deep web est primordiale pour protéger la marque d'une entreprise contre la fraude et le phishing.

Pourquoi Orange ?

- **Plus de 2100 cyber-experts dans le monde entier**
- **16 SOC, 10 CyberSOC et 4 CERT**
- **Base de données propriétaire de Threat Intelligence en temps réel**
- **Capacités de service Follow-the-Sun 24/7**
- **CERT, Signal Intelligence and Behavior labs pour qualifier et contrer les menaces émergentes**
- **Plus de 3700 clients en France et à l'internationnal**

Orange Cyberdefense

Pour en savoir plus :
https://cyberdefense.orange.com/fr/