HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE

RENFORCER LA SÉCURITÉ DE VOTRE CHAÎNE D'APPROVISIONNEMENT

Dans ce document d'information, nous analysons les vulnérabilités des chaînes d'approvisionnement et expliquons comment la mise en place d'une culture de sécurité solide par le biais d'une formation continue à la sensibilisation à la sécurité est essentielle pour garantir la sécurité des données des fournisseurs de services et de toutes les autres entreprises pour lesquelles ils fournissent des services.

Les organisations modernes s'appuient sur un large éventail de composants matériels, d'applications logicielles et de services cloud, toutes provenant de multiples fournisseurs. Cette interdépendance crée plusieurs points de risque :

- **Réseaux de fournisseurs complexes : Chaque fournisseur, qu'il s'agisse de pièces physiques ou de composants logiciels, est une porte d'entrée potentielle pour une attaque.**
- **Phishing et ingénierie sociale : Les attaquants utilisent souvent des méthodes de phishing complexes pour compromettre les fournisseurs et cibler ensuite leurs clients.**

EXEMPLES CONCRETS

Attaques du NHS et de Change Healthcare

Les perturbations des services essentiels ont eu des répercussions considérables. Des attaques récentes ont paralysé les diagnostics du NHS par le biais d'un ransomware (Synnovis) et ont massivement perturbé les opérations de Change Healthcare.

Incident SolarWinds

Une violation très médiatisée qui a montré comment des mises à jour compromises peuvent permettre aux attaquants de prendre pied dans des réseaux par ailleurs sécurisés. Les services de renseignement russes ont modifié une mise à jour SolarWinds Orion, infiltrant de nombreuses organisations par le biais du correctif malveillant.

3CX en Corée du Nord

Des pirates nord-coréens ont mené une attaque en plusieurs étapes en 2023, compromettant 3CX par le biais d'un logiciel tiers sur le PC d'un employé. Cela a permis la distribution mondiale d'une mise à jour malveillante de 3CX.

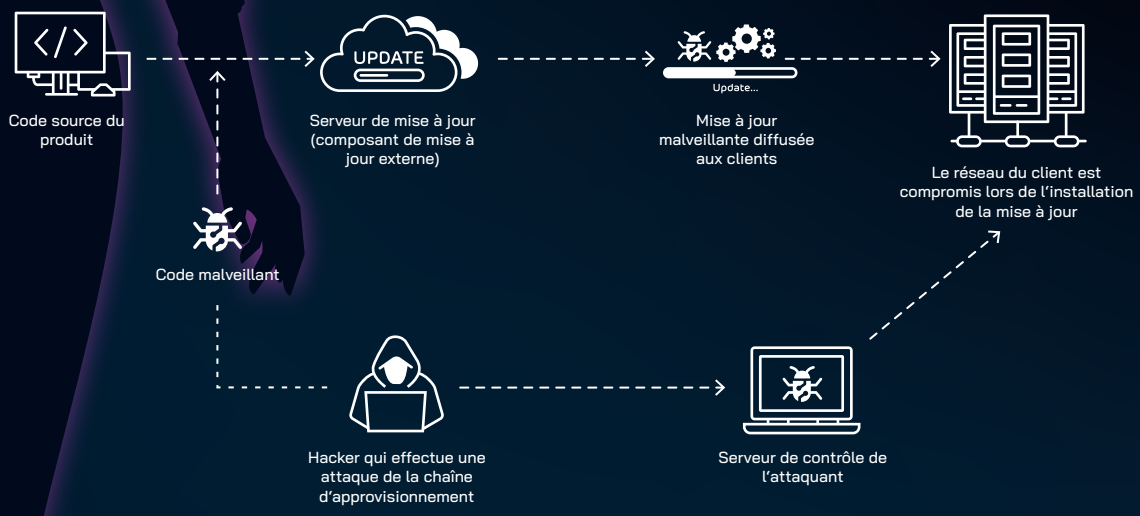
HORNETSECURITY

INFO
SHEET

ANATOMIE D'UNE ATTAQUE CONTRE LA CHAÎNE D'APPROVISIONNEMENT

Il est essentiel de comprendre le fonctionnement de ces attaques :

- **Compromettre le fournisseur : les cybercriminels s'infiltrent chez un fournisseur de confiance par le biais de dépendances tierces ou de mécanismes de mise à jour.**
- **Injection de code malveillant : Une fois dans le système du fournisseur, les attaquants insèrent un code nuisible qui agit comme une porte dérobée.**
- **Distribution aux clients : La mise à jour malveillante est ensuite transmise aux utilisateurs finaux, compromettant ainsi leurs systèmes.**
- **Vol de données et perturbation : En accédant à l'organisation cible, les attaquants peuvent voler des données et perturber les opérations.**



L'IMPÉRATIF DE SENSIBILISATION À LA SÉCURITÉ

Dans les chaînes d'approvisionnement, il est important de se rappeler que ce n'est pas seulement la sécurité des données d'un fournisseur de services qui est en jeu, mais celles de toutes les entreprises auxquelles il s'adresse. Même les protections techniques les plus complexes peuvent être sapées par l'erreur humaine. La cyber résilience ne consiste pas seulement à déployer des technologies de pointe, mais aussi à instaurer une culture de la sécurité.

- **Responsabilisez votre équipe : former les employés à reconnaître les tentatives de phishing et autres tactiques d'ingénierie sociale est votre première ligne de défense.**
- **Amélioration continue : Une formation régulière et automatisée aide les employés à rester vigilants et à suivre l'évolution des menaces.**

09-25

HORNETSECURITY

INFO
SHEET

SECURITY AWARENESS SERVICE: VOTRE BOUCLIER CONTRE LES MENACES DE LA CHAÎNE D'APPROVISIONNEMENT

Le Security Awareness Service de Hornetsecurity est conçu pour combler le fossé entre les défenses techniques et les vulnérabilités humaines :

- **L'indice de sécurité des employés (ESI) : L'évaluation des profils de risque individuels et l'adaptation de la formation pour répondre aux besoins spécifiques.**
- **Formation automatisée et continue : Des exercices de simulation d'hameçonnage et des contenus éducatifs sont proposés en continu afin d'améliorer la vigilance au fil du temps.**
- **Faible coût administratif : Intégration transparente dans votre cadre de sécurité existant, libérant des ressources tout en garantissant une protection solide.**
- **Des résultats probants : L'amélioration de la culture de sécurité entraîne une réduction des incidents de phishing et d'autres attaques d'ingénierie sociale, protégeant ainsi l'ensemble de votre chaîne d'approvisionnement.**

PRINCIPAUX AVANTAGES

Réduire l'exposition :

atténuer les risques de manière proactive en formant les employés aux nouvelles menaces.

Renforcer les relations avec les fournisseurs:

démontrer un engagement en matière de sécurité qui rassure les partenaires et les clients.

La résilience en action:

Assurer la continuité de l'activité même en cas d'attaques complexes de la chaîne d'approvisionnement.

Avantage concurrentiel :

Tirez parti d'une main-d'œuvre bien formée pour vous différencier sur le marché.

Donnez à votre équipe les moyens de se défendre contre les cybermenaces !

EN SAVOIR PLUS !

09/25