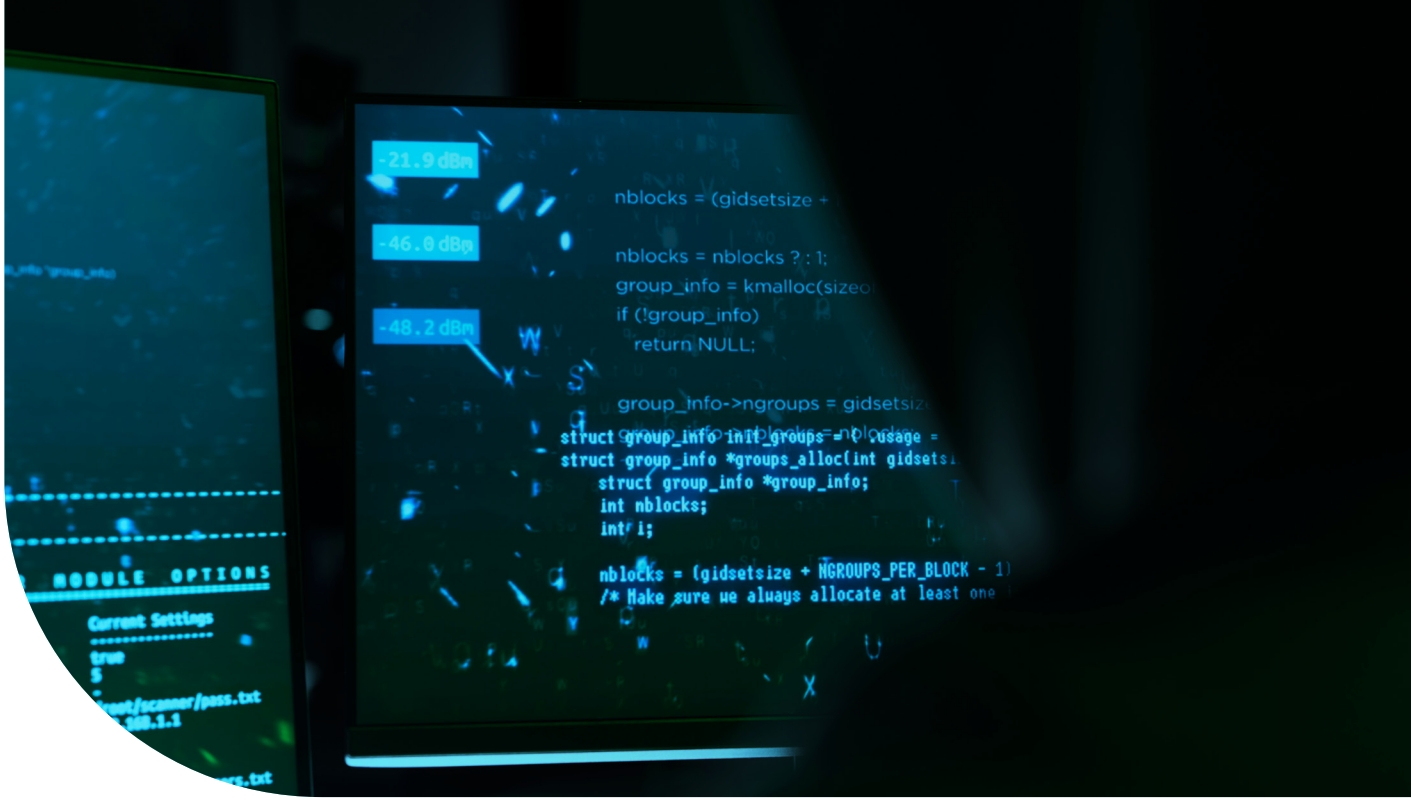
PLAN D'URGENCE INFORMATIQUE

Comment se préparer à une cyberattaque

ESET

Digital Security

Progress. Protected.



Tous les ordinateurs se mettent soudain en veille, le site web est hors service, et aucun de vos collaborateurs ne peut accéder au réseau ou aux données. Toute l'informatique s'est soudainement arrêtée. Il s'avère qu'il en sera ainsi pendant quatre semaines car l'entreprise ne s'est pas préparée à ce type d'incident. De nombreuses organisations, notamment les petites et les moyennes entreprises, ne sont pas préparées aux crises causées par des cybercriminels. Que faire en cas de cyberattaque ?

Bien que le nombre de cyberattaques ait augmenté ces dernières années, et que la pandémie de COVID-19 ait même accéléré la tendance, cette question est encore sous-estimée par de nombreuses entreprises. Selon l'enquête CNBC | Momentive sur les petites entreprises de Q3 2021, 56 % des propriétaires de petites entreprises américaines ont déclaré qu'ils ne s'inquiétaient pas d'être victimes d'un piratage informatique au cours des 12 prochains mois, et 24 % ont déclaré qu'ils n'étaient « pas du tout inquiets ».

De plus, seulement 28 % des petites entreprises ont déclaré avoir mis en place un plan d'intervention en cas de cyberattaque, 42 % ont déclaré ne pas avoir de plan, et 11 % ont révélé qu'elles n'étaient « pas sûres » d'avoir un plan en place.

13 %

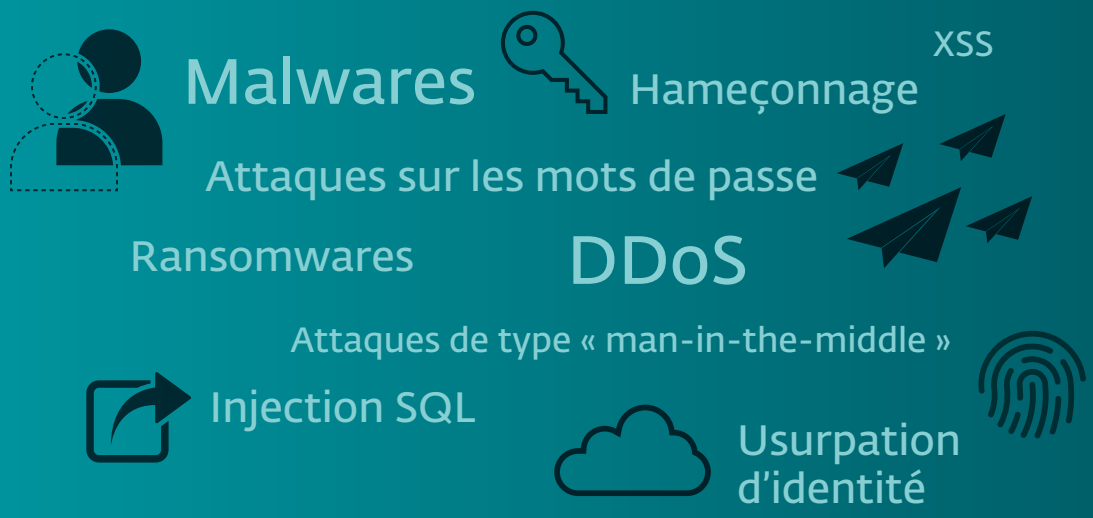
Proportion de petites entreprises qui forment leur personnel à la cybersécurité. Seules 19 % d'entre elles ont testé la réactivité de leur personnel, par exemple en effectuant des exercices d'hameçonnage simulé.

Source : Enquête de 2021 d'Ipsos MORI et du ministère britannique du numérique, de la culture, des médias et du sport

Les experts qualifient ce comportement de négligent. Il ne s'agit plus de savoir si, mais quand les cyberattaques vont se produire. Cela a été confirmé par une enquête publiée en 2021 par l'association numérique allemande Bitkom.

9 sur 10

Près de 90 % des 1 000 entreprises de tous les secteurs interrogées en Allemagne ont déclaré avoir été touchées par des cyberattaques. Quels types d'attaques ont été le plus souvent mentionnés ?



86 %

des entreprises ont subi des dommages causés par une cyberattaque. En 2019, ce chiffre n'était que de 70 %.

Source : Bitkom Research, Allemagne, comparaison des enquêtes de 2019 et 2021

Création d'un plan d'urgence efficace

Les experts en médecine intensive et d'urgence appellent la phase décisive des blessures ou des maladies mortelles l'« heure d'or ». Plus forte la réactivité, plus les chances d'un rétablissement complet sont élevées. Une gestion professionnelle de la continuité des activités est une condition préalable pour passer le cap de l'heure d'or dans un contexte opérationnel. **L'objectif est d'accroître la fiabilité des processus et de réagir rapidement et systématiquement en cas d'urgence,** notamment en cas d'attaques de pirates et de malwares.

Le plan d'urgence, également appelé gestion des incidents informatiques. Il s'agit généralement de l'ensemble du processus organisationnel et technique de traitement des incidents ou des dysfonctionnements de sécurité détectés ou suspectés dans les domaines informatiques, ainsi que des mesures et des processus préparatoires. L'éventail des incidents possibles s'étend des problèmes techniques et des points faibles jusqu'aux attaques spécifiquement dirigées contre l'infrastructure informatique. La gestion des incidents informatiques au sens strict doit **prendre en compte tous les détails organisationnels, juridiques et techniques**.

La probabilité que les pirates réussissent une attaque est extrêmement élevée. Les cybercriminels eux-mêmes sont désormais très professionnels. Ils ont aujourd'hui à leur disposition différents moyens rentables de manipuler les gens et propager des chevaux de Troie, des virus, etc. dans le réseau. **Les cyberattaques ne sont pas toujours immédiatement découvertes** car tous les niveaux du système ne sont pas toujours supervisés.

Une bonne préparation est cruciale pour la création d'un plan d'urgence. En effet, en cas de scénario catastrophe, la chose la plus importante à faire est de **réagir rapidement**, stopper l'attaque le plus rapidement possible, protéger les données stockées et rétablir le fonctionnement normal de l'entreprise dans les meilleurs délais. Différentes mesures immédiates doivent donc être définies, par exemple, lorsque l'ensemble du réseau de

communication s'effondre, que les sites web ne sont plus disponibles ou même que l'ensemble du processus de production s'arrête après une attaque.

Que faire lors de l'élaboration d'un plan d'urgence ?

- **Créez un plan d'urgence opérationnel :** Consignez toutes les mesures nécessaires qui doivent être prises en cas d'urgence. Il est préférable de demander l'avis d'experts. Il est possible de trouver une première ébauche dans des modèles types.
- **Désignez un responsable de la sécurité informatique :** Nommez une personne responsable pour traiter les questions de sécurité dans l'entreprise. Depuis l'introduction du RGPD, les entreprises de plus de 10 employés doivent désigner un délégué à la protection des données.
- **Vérifiez votre plan d'urgence actuel :** Si vous disposez déjà d'un plan d'urgence, vous devriez le faire vérifier et le mettre en œuvre par des experts. Vous devriez également vous assurer que votre plan d'urgence est compréhensible pour les profanes.
- **Préparez votre entreprise à toutes les éventualités :** Pour savoir réellement si le plan fonctionne, vous devez le tester à l'avance en pratique.

Cyberattaque : que faire en cas de crise

Au fil du temps, les cybercriminels causent de plus en plus de dégâts, infiltrant l'architecture informatique jusqu'au moindre élément, ou siphonnant des données extrêmement sensibles. Les responsables informatiques ont donc pour mission de reconnaître les activités nuisibles à un stade précoce et d'agir rapidement. C'est le seul moyen de minimiser les dommages causés, voire d'éviter la défaillance totale du système dans son ensemble. Outre les conséquences financières, les entreprises doivent avant tout craindre une énorme perte d'image de marque et de confiance de la part des clients. Alors, que doivent faire les entreprises lorsque des criminels ont détourné leurs données et que les communications ne fonctionnent plus ?

Où s'adresser en cas de cyberattaque ?

- Les prestataires de services managés (MSP), les détaillants informatiques et les fournisseurs de système ont une grande expérience des cyberattaques et peuvent fournir une assistance rapide et ciblée.

- En cas d'attaque, vous avez la possibilité d'obtenir de l'aide en France grâce au dispositif Cybermalveillance.gouv.fr. Il s'agit d'un portail d'assistance et de prévention du risque numérique géré par l'Etat Français au sein duquel vous trouverez de l'aide pour les entreprises et des moyens de vous aider concrètement dans vos démarches à l'aide de professionnels homologués et spécialisés dans la cybersécurité.

9 conseils pour vous aider à réduire au minimum l'impact d'une cyberattaque

1. Gardez votre calme et agissez de manière tactique

Lorsqu'un logiciel de sécurité informatique tire la sonnette d'alarme, la première chose à faire est de garder son calme. Une cyberattaque réussie est souvent une surprise. Un malware peut par exemple se cacher dans le réseau pendant des semaines sans être remarqué si le service informatique ne surveille pas tous les niveaux du système. Mais lorsqu'un incident se produit, il est important de prendre les bonnes décisions dans les plus brefs délais. Sans un plan d'urgence avec des mesures immédiates définies, le chaos peut rapidement s'ensuivre.

2. Déterminez l'étendue de l'infection

De nombreux services informatiques d'entreprises victimes d'attaques de malwares se fient à leur intuition plutôt qu'à une analyse approfondie pour déterminer les conséquences de ces attaques. Il est bien sûr important de réagir, mais pas sur la base d'hypothèses. Lorsqu'une entreprise dispose d'un plan opérationnel de gestion des urgences informatiques, le département informatique peut rapidement trouver les bonnes réponses aux questions centrales :

- ☑ Quels systèmes ont été infectés ?
- ☑ Comment cela s'est produit ?
- ☑ Des données critiques pour l'entreprise ont-elles été perdues ?
- ☑ L'infection affecte-t-elle uniquement des composants individuels, ou un sous-réseau entier ?
- ☑ Les informations des clients et les données des employés sont-elles tombées entre les mains des attaquants ?

3. Assurez les opérations informatiques

Lorsque des informations internes sont tombées entre les mains de personnes non autorisées, les employés et les clients concernés doivent d'abord être informés. Si les systèmes informatiques ont été gravement touchés par une attaque, il convient d'activer des systèmes de sauvegarde et des connexions réseau redondantes, car les activités ne doivent pas souffrir d'une cyberattaque. Pour ce faire, un plan d'urgence est également nécessaire afin d'accélérer la réactivité.

4. Endiguez l'infection

Les systèmes informatiques infectés doivent être isolés. Afin d'empêcher la propagation de l'infection dans le réseau, le service informatique peut déconnecter les segments réseau dans lesquels se trouvent les ordinateurs infectés. Cela signifie que les attaquants n'auront plus accès à ces systèmes et ne pourront pas « siphonner » de données utilisables.

Dans tous les cas, le service informatique doit essayer de déchiffrer le trafic de données chiffré entre les systèmes informatiques infectés de son propre réseau et les ordinateurs des attaquants. Cela leur permettra de déterminer si d'autres ordinateurs du réseau ont été contaminés, et quelles règles de pare-feu sont nécessaires pour empêcher tout accès non autorisé. Ces contre-mesures peuvent être mises en œuvre beaucoup plus rapidement et plus efficacement lorsqu'une entreprise utilise une solution de sécurité informatique, par exemple, les nouvelles solutions professionnelles d'ESET.

5. Protégez les preuves

Les preuves des incidents doivent être conservées pour permettre aux forces de police de prendre des mesures après une attaque réussie. Une documentation complète peut également vous aider à faire valoir vos droits sur une police d'assurance existante.

6. Éliminez l'infection et empêchez d'autres attaques

L'une des tâches les plus exigeantes consiste à nettoyer les systèmes informatiques touchés et mettre un terme à toute nouvelle attaque de la même manière. Un logiciel antivirus ou antimalwares qui nettoie automatiquement les systèmes informatiques est un outil utile pour ce faire. Afin d'empêcher de

nouvelles attaques du même type, il convient d'éliminer les failles de sécurité qui ont rendu ces activités possibles. Pour en être absolument sûr, il est conseillé d'analyser les paquets de données qui sont transportés sur le réseau, en particulier pour y rechercher les commandes et les schémas précédemment utilisés par les attaquants.

D'autres précautions de sécurité consistent à vérifier les règles du pare-feu et modifier les mots de passe que les employés utilisent pour se connecter au réseau. Une analyse plus approfondie de la cyberattaque mérite d'être envisagée, car, dans de nombreux cas, les attaques individuelles font partie de menaces persistantes avancées (APT). Il s'agit de cyberattaques ciblées, complexes et continues sur les PME ou leurs employés. Lorsque la direction devient la cible de ces APT, on peut supposer que d'autres attaques suivront.

7. Législation – RGPD et autres réglementations pertinentes

Des questions juridiques se posent après une cyberattaque. Elles devraient être clarifiées à l'avance. Depuis l'introduction du RGPD, certains incidents doivent être signalés aux autorités dans un certain délai. Les obligations en matière d'information doivent être clarifiées au préalable avec votre service juridique, afin que votre entreprise reste conforme à la législation et n'ait pas à payer d'amendes supplémentaires par la suite.

8. Ne payez pas en cas d'attaque de ransomware

Les ransomwares sont un moyen d'attaque couramment utilisé par les cybercriminels. Ils chiffrent les données des victimes et les pirates exigent ensuite une rançon pour les restituer. Ne payez jamais la rançon demandée, car vous n'avez pas l'assurance de pouvoir récupérer vos données. Lorsque vous exprimez votre volonté de payer, vous validez ainsi ce modèle de financement du cybercrime et invitez les pirates à poursuivre leur chantage.

9. Tirez les leçons des cyberattaques et des erreurs

Il est important que les entreprises tirent les bonnes conclusions de l'analyse des attaques et prennent les précautions appropriées. Toute vulnérabilité précédemment inconnue qui a été corigée représente en fin de compte une opportunité d'améliorer les mesures défensives au périmètre du réseau de l'entreprise et de fermer les points d'entrée potentiels. Il est également crucial que le responsable informatique surveille attentivement tous les niveaux du système. Cela facilite la détection d'une cyberattaque à un stade précoce, et ne donne pas aux intrus l'occasion de s'infiltrer dans des zones spécifiques pour scruter le système avant de déclencher l'attaque proprement dite.

En cas de cyberattaque, veillez à ce que :

- Aucun autre dommage ne puisse résulter de l'attaque.
- Des mesures immédiates puissent être prises en cas de crise sans impliquer la direction afin de ne pas perdre de temps à devoir obtenir une approbation.
- Les données de connexion puissent être modifiées immédiatement. Les mots de passe et les identifiants volés ainsi que les comptes de messagerie contaminés peuvent causer d'autres dommages à l'avenir. Votre plan d'urgence doit donc inclure une stratégie sur la manière de procéder après une attaque de pirates informatiques impliquant les données d'accès appartenant à l'entreprise.
- Même les accès invités, s'ils existent, soient désactivés et le réseau mis hors ligne. Les appareils invités non gérés, en particulier, présentent un risque élevé de pénétration de malwares dans le système.
- Aucun email ne soit ouvert, qu'aucun appareil mobile ne soit connecté au réseau de l'entreprise ou à d'autres réseaux, par exemple les réseaux des clients, et que tous les supports de stockage connectés au réseau, tels que les clés USB, les disques durs externes, les appareils photo, etc. soient déconnectés et ne soient ni utilisés ni sortis du lieu de travail.

5 conseils supplémentaires pour améliorer la sécurité

Si vous prenez les mesures énumérées ci-dessus, vous êtes déjà très bien préparé à une crise. Voici cinq autres recommandations qui vous aideront à optimiser la sécurité de votre entreprise :

1. Automatisez autant que possible

Dans le meilleur des cas, le plan d'urgence peut être largement automatisé et peut utiliser des outils modernes. Tous les processus qui peuvent être exécutés de manière autonome réduisent la charge de l'administrateur. Ces actions peuvent inclure, par exemple, l'encapsulation automatique des endpoints affectés. Les pare-feux sur les endpoints coupent toutes les connexions sauf celles de l'administration à distance.

2. Surveillez la journalisation et la documentation

Il est également important que toutes les étapes des actions soient entièrement consignées et documentées, qu'elles soient automatiques ou manuelles. C'est le seul moyen de suivre rétrospectivement le processus d'infection et d'adapter le plan d'urgence en conséquence, notamment afin de combler les éventuelles failles de sécurité et modifier les comportements humains.

3. Effectuez régulièrement des sauvegardes

Quelle que soit la cause de l'incident de sécurité, la capacité des entreprises à rétablir le plus rapidement possible les données perdues et essentielles à leur activité est cruciale. Cela commence par des sauvegardes régulières. Ici aussi, la sauvegarde automatique des données est un bon choix, car elle garantit la cohérence des informations et veille à ce que les employés n'oublient pas de faire des sauvegardes. Les sauvegardes doivent être effectuées sur au moins deux supports externes, et une version chiffrée dans un stockage Cloud doit également être envisagée (vous devriez choisir un lieu de stockage en Europe pour des questions de protection des données). Là encore, les systèmes de sauvegarde et de récupération doivent être testés régulièrement.

4. Utilisez un outil de détection et de traitement sur les endpoints (EDR)

Un outil d'EDR permet la surveillance constante et complète de toutes les activités des endpoints. Les processus suspects peuvent alors être analysés en détail, et les responsables informatiques peuvent réagir aux menaces à un stade précoce. Les entreprises améliorent considérablement leurs mesures de sécurité grâce à l'utilisation de la technologie EDR, particulièrement en cas d'attaques zero-day et de ransomware, d'attaques ciblées (menaces persistantes avancées) ou d'infraction des politiques internes de l'entreprise.

5. Révisez régulièrement votre plan d'urgence

Tout comme les exercices de lutte anti-incendie, les plans d'urgence informatiques doivent être testés régulièrement. Rien n'est plus fatal que de se fier à un plan qui, en fin de compte, ne fonctionne pas.

Conclusion

La contamination des PC, des serveurs ou des systèmes mobiles par des malwares peut constituer une menace sérieuse pour les entreprises, notamment lorsque des informations internes tombent entre les mains des attaquants. De tels incidents attirent cependant l'attention des responsables sur deux éléments importants : d'une part, sur les mesures de sécurité informatique qui doivent être optimisées, et d'autre part sur le fait qu'un plan d'urgence actualisé peut minimiser les dommages.

Quand la technologie engendre le progrès, ESET est là pour le protéger.

Depuis plus de 30 ans, ESET® développe des logiciels et des services de sécurité informatique pour protéger le patrimoine numérique des entreprises, les infrastructures critiques et les consommateurs du monde entier contre des cybermenaces. Nous protégeons les terminaux fixes et mobiles, les outils collaboratifs, et assurons la détection et le traitement des incidents. Établis dans le monde entier, nos centres de R&D récoltent et analysent les cybermenaces pour protéger nos clients et notre monde numérique. Pour plus d'informations, consultez le site www.eset.com/fr/ ou suivez-nous sur LinkedIn, Facebook et Twitter.

+110 000 000
Utilisateurs protégés dans le monde entier

+300 000
Nouveaux échantillons uniques de malwares détectés quotidiennement

+600
Experts en recherche et en développement

+400 000
Clients professionnels dans +200 pays et territoires