Empêcher la cybercriminalité

Mode d'emploi à l'intention des petites et moyennes entreprises

Impressum

Police cantonale bernoise et Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) sur mandat du Réseau national de soutien aux enquêtes dans la lutte contre la criminalité informatique (NEDIK). Contact: Police cantonale zurichoise, NEDIK, Zurich, cyc_nedik@kapo.zh.ch

Photographies: mises à disposition par la Police cantonale zurichoise.

Ihre **POLIZEI**
Votre **POLICE**
La vostra **POLIZIA**

Kantonale und Städtische Polizeikorps
Corps de police cantonaux et municipaux
Corpi di polizia cantonali e comunali

Table des matières

1 Les cyberattaques coûtent cher, à vous aussi

La numérisation offre à l'économie de nouvelles opportunités de croissance et d'emploi. Toutefois, cela signifie également une dépendance accrue envers une infrastructure informatique en état de fonctionner. C'est ce qu'exploitent les criminels. Tout le monde est concerné: de l'entreprise artisanale aux grandes firmes employant plusieurs milliers de personnes. Environ 40 pourcent des entreprises suisses ayant participé à un sondage[1] ont indiqué avoir été victimes de cybercriminalité, allant de la mise hors ligne d'un site internet à des dommages portant sur l'ensemble du réseau entrepreneurial. Les entreprises essuient le plus souvent des préjudices financiers, et dans certains cas des informations confidentielles peuvent également être rendues publiques.

On peut se protéger contre de nombreux cyberrisques.

La police et la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) vous donnent ci-après des recommandations concrètes pour vous protéger contre la cybercriminalité et vous montrent comment réagir en cas d'attaque. De plus, si vous avez été victime d'incidents importants, nous voulons vous inciter à les dénoncer à la police. Car seul un rapprochement des autorités de poursuite pénale et de l'économie permet d'identifier les pirates informatiques, de les condamner et ainsi de combattre durablement la cybercriminalité.

Vous trouvez des informations plus détaillées relatives à votre sécurité informatique sur www.melani.admin.ch

1 «Sondage mondial de 2018 sur la fraude et les crimes économiques – Les conclusions suisses», PwC, 2018.

2 Comment vous soutirent-ils de l'argent?

Pour leurs cyberattaques, les pirates suivent souvent les mêmes modèles et emploient toujours les mêmes moyens. Ceux-ci peuvent se répartir en trois catégories: chantage, escroquerie et usage abusif des données.

2.1 Comment exercent-ils un chantage sur vous?

Les maîtres-chanteurs attaquent l'infrastructure informatique de leurs victimes dans le but de leur soutirer de l'argent. Ils cherchent à déranger, voire à stopper, le plus grand nombre possible de processus dans l'entreprise. Les victimes sont contactées et doivent verser un certain montant afin que le piratage cesse ou que des données volées ne soient pas publiées.

Les pirates connaissent le type et la grandeur de l'entreprise qu'ils attaquent.

Rançongiciel (ransomware)	Des logiciels malveillants sont envoyés en grand nombre, par exemple par courriel, afin de voler des informations et des mots de passe. Les victimes ainsi trouvées sont ensuite espionnées afin de récolter des informations. En cas de succès, les pirates prennent le contrôle du système informatique et commencent à crypter les données de l'entreprise. Le cas échéant, des données seront également volées. Les maîtres-chanteurs exigent une rançon (angl. ransom) afin de décrypter les données.
DDoS (déni de service distribué)	Un système accessible depuis internet est surchargé par un très grand nombre de demandes, de sorte qu'il ne peut plus fonctionner. Pour faire cesser l'attaque, il faut payer une rançon. Les pirates peuvent également être des groupuscules voulant porter atteinte à l'entreprise ou à l'organisation, ou des concurrents souhaitant se ménager un avantage commercial.
Publication de données	Les maîtres-chanteurs menacent de publier des données qu'ils ont au préalable volées à l'entreprise, au cas où aucune rançon ne serait versée.

2.2 Comment vous escroquent-ils?

Les escrocs induisent leurs victimes en erreur, afin que celles-ci fassent quelque chose qu'elles ne feraient pas d'elles-mêmes. À cet effet, ils choisissent souvent un scénario qui éveille si possible beaucoup d'émotions chez la personne visée ou qui lui est familier, créant ainsi un faux sentiment de sécurité.

Les pirates s'informent au préalable de multiples manières sur la structure de l'entreprise, à l'aide d'informations accessibles (p.ex. sur le site internet de l'entreprise ou les réseaux sociaux). Ils cherchent ensuite une «cible» qu'ils confrontent à un scénario sur mesure. Cette méthode s'appelle manipulation sociale (social engineering). Son objectif est que la victime accomplisse des actions pilotées par les escrocs sans le remarquer.

Hiérarchie	Les criminels exploitent la structure hiérarchique d'une entreprise pour forcer à agir. Ils simulent par exemple une identité et exigent d'un collaborateur ou d'une collaboratrice, au nom de la hiérarchie, de partager des informations sensibles ou de faire un versement.
Urgence	Les pirates font croire à la victime qu'elle doit agir en toute hâte.
Convoitise/curiosité	Les escrocs promettent à la victime un gain ou une surprise si elle ouvre le fichier ou clique sur un lien.
Peur/colère	Les pirates menacent la victime, au cas où elle n'exécuterait pas l'ordre, ou font des déclarations manifestement inexactes, que l'on peut corriger en cliquant sur un lien.
Sympathie	Le thème présenté fait vibrer la corde sensible de la victime. Celle-ci veut s'associer afin de régler un problème.

2.3 Comment utilisent-ils abusivement vos données?

Souvent de l'argent est retiré d'un compte de la victime à l'aide d'un logiciel malveillant. Mais on peut gagner de l'argent également en volant des données d'accès et en les vendant sur le marché noir.

Parfois les données rentables de l'entreprise sont également visées. Il s'agit ici surtout des secrets commerciaux ou des données de la clientèle. Si votre entreprise enregistre les données d'accès de votre clientèle, voire des données de carte de crédit, celles-ci sont d'un grand intérêt pour les criminels.

Les données stockées devraient faire l'objet d'une sauvegarde spéciale (cryptées).

Chevaux de Troie	Les chevaux de Troie spécialisés en cyberbanque sont des programmes permettant aux pirates d'avoir accès à votre compte cyberbancaire. Ils sont souvent envoyés par courriel (p.ex. camouflés en facture ou publicité).
Fuite de données	Les pirates réussissent à accéder à votre réseau entrepreneurial. Ils y trouvent des données précieuses, qu'ils copient. Ils peuvent ensuite soit les vendre à des tiers ou vous faire du chantage en menaçant de les publier.
Hameçonnage	L'hameçonnage (phishing) est une technique visant à se procurer des données confidentielles. Elle se pratique via courriel, site internet, téléphonie par internet ou SMS. Les destinataires sont avertis que leurs données d'accès ne sont plus sûres ou plus actuelles et qu'il faudrait les modifier via le lien donné. Ce lien mène cependant à un site internet falsifié. Les victimes s'y connectent, ce qui permet aux pirates d'obtenir les données d'accès et de commander par exemple des marchandises sur facture.

3 Comment pouvez-vous protéger votre entreprise?

Des mesures techniques et organisationnelles sont nécessaires pour éviter une attaque. Elles ne peuvent être déléguées aux collaboratrices ou collaborateurs, mais doivent être prises et coordonnées par la direction.

Les mesures contre les cyberattaques doivent être prises par la direction.

3.1 Mesures techniques

> **Procéder à des mises à jour de sécurité**
Un vieux logiciel est une porte ouverte prisée pour les logiciels malveillants. Assurez-vous que des mises à jour de sécurité s'effectuent automatiquement sur l'ensemble des ordinateurs et serveurs de votre réseau. De même, actualisez régulièrement les logiciels tiers tels qu'Adobe Reader, Adobe Flash et Java ainsi que les appareils tels qu'imprimante, routeur, etc.

Si votre entreprise dispose d'un site internet et s'il repose sur un système de gestion de contenu (Content Management System, CMS), assurez-vous que celui-ci soit toujours actualisé. La plupart des CMS offrent une fonction de mise à jour automatique et simple à activer.

> **Protéger le réseau**
Utilisez un pare-feu (firewall): vous devriez doter chaque ordinateur d'un pare-feu personnel. De plus, protégez le réseau entrepreneurial contre les incursions venant d'internet à l'aide d'un pare-feu. Par défaut, le pare-feu devrait bloquer l'ensemble des transferts, sauf s'ils sont autorisés par des règles.

Répartissez votre réseau entrepreneurial en différents secteurs: un réseau séparé pour la production, un autre pour les ressources humaines et un troisième pour la comptabilité. Il n'y a aucune raison que le personnel des ressources humaines ait accès à votre site de production. Vous évitez ainsi par exemple que l'ordinateur qui pilote votre usine et n'est plus actualisable devienne une porte ouverte aux pirates.

Sécurisez votre accès à distance: l'accès extérieur à votre réseau ne devrait jamais être protégé par une simple authentification (nom d'utilisateur et mot de passe). Utilisez au moins une authentification à deux facteurs ou installez une liaison plus sûre via un réseau privé virtuel (VPN). C'est également valable pour l'accès de services informatiques ou d'administrateurs externes.


PASSWORD

> **Sauvegarder les données**
Définissez un processus réglant la sauvegarde régulière de vos données et respectez-le systématiquement. Évaluez la quantité de données en nombre de jours que vous pouvez supporter de perdre et stockez en conséquence une copie supplémentaire de votre sauvegarde séparément (offline) et hors murs (offsite). Exercez-vous de temps en temps à restaurer une sauvegarde, afin que ce processus vous soit familier en cas de besoin. Assurez-vous de conserver les sauvegardes antérieures durant plusieurs mois.

> **Installer une protection antivirale**
Assurez-vous qu'un logiciel antivirus soit installé sur chaque ordinateur et le protège en temps réel. Veillez également à ce qu'il soit actualisé régulièrement et qu'il effectue chaque jour un examen complet du système.

> **Utiliser avec prudence les services de cybernuage**
Montrez-vous prudent(e) en utilisant des services de cybernuage (cloud), employés par de nombreux programmes. Demandez-vous quelles données doivent être enregistrées localement et quelles autres dans le nuage. Les données sensibles et les secrets commerciaux ne devraient jamais être archivés non cryptés dans le cybernuage.

La prudence est importante!
Réfléchissez au préalable aux mesures qui doivent être prises en cas d'attaque. Définissez quels fichiers journaux (qui regroupent de façon chronologique l'ensemble des événements survenus sur un système informatique) sont enregistrés et combien de temps. Ordinateurs et serveurs peuvent enregistrer tous les processus informatiques importants ou les données de liaison à autres ordinateurs, idéalement en un endroit centralisé. D'amples données du journal aident non seulement les autorités de poursuite pénale dans leurs enquêtes, mais aussi les entreprises à connaître l'origine de l'attaque, à obtenir des informations sur les systèmes infectés dans leur propre réseau et à prendre des mesures correctives appropriées. Au cas où votre réseau est géré par une entreprise informatique, nous vous recommandons de clarifier les questions relatives aux fichiers journaux et à la détection des piratages. Il est également recommandé d'établir un inventaire complet et à jour des systèmes, logiciels et réseaux.

3.2 Mesures organisationnelles

> **Régler l'utilisation des informations de l'entreprise**
Définissez des directives régissant la transmission des informations de votre entreprise. Demandez-vous exactement quelles informations vous voulez publier par exemple sur votre site internet ou sur les réseaux sociaux, car celles-ci sont collectées par les criminels. En principe, aucune information confidentielle ne devrait être transmise par voie anonyme (p.ex. téléphone ou courriel).

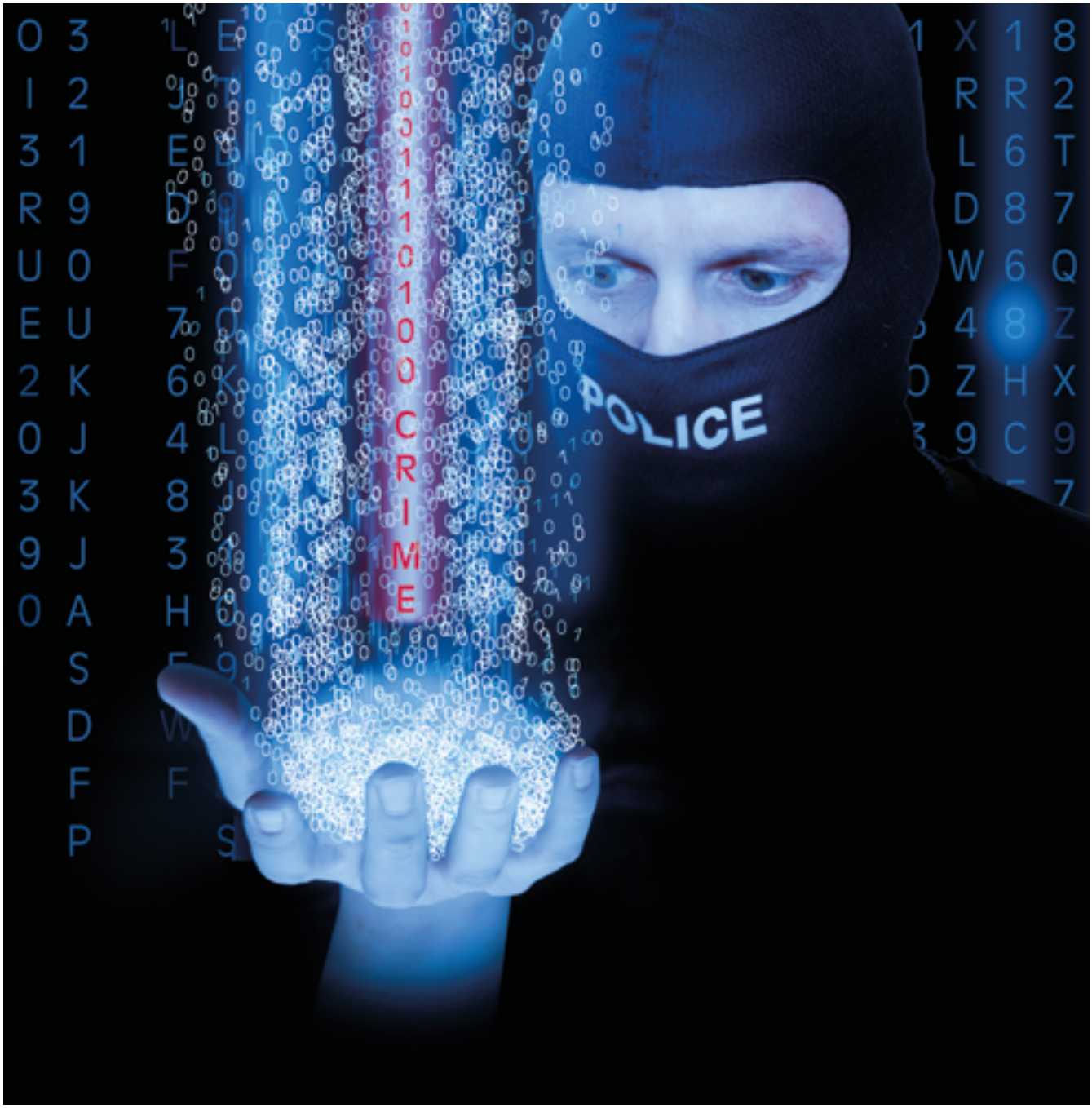
> **Sensibiliser le personnel à l'utilisation des courriels**
Les logiciels malveillants atterrissent souvent dans votre ordinateur via des annexes déguisées en pseudo-factures. Cultivez une saine méfiance: n'hésitez pas à en vérifier l'authenticité par téléphone et incitez votre personnel à faire de même. Il faut absolument vous assurer qu'aucune macro de documents Microsoft d'origine inconnue ne puisse être exécutée.

> **Utiliser des mots de passe sûrs et ne pas les transmettre**
Définissez des règles contraignantes pour les mots de passe et appliquez-les de manière systématique. Les mots de passe devraient comporter à la fois lettres, chiffres et caractères spéciaux, soit douze signes au minimum. Misez sur une authentification à deux facteurs partout où c'est possible. Évitez absolument d'utiliser les mêmes mots de passe à différents endroits! Pour ce faire, ayez recours à un gestionnaire de mots de passe et générez un mot de passe par application. Il existe sur le marché différents programmes de gestion en fonction des systèmes d'exploitation et des appareils. Ces programmes sont gratuits ou soumis à une licence. Ne transmettez jamais des mots de passe ou des données d'accès par téléphone ou courriel.

> **Régler l'accès aux données**
Normalement votre personnel ne devrait disposer d'aucun droit d'administrateur. Il s'agit de ne donner à chaque personne que les droits dont elle a besoin pour accomplir son travail.

> **Protéger les comptes cyberbancaires**
Pour vos payements, utilisez un ordinateur séparé sur lequel vous ne pouvez pas surfer sur internet ni recevoir de courriels. L'ensemble des processus concernant le trafic des payements devrait être clairement réglé à l'interne et dans tous les cas respecté par le personnel, par exemple le principe du double contrôle et la signature collective. De plus, avant d'être libérés, les payements doivent être visés par un/e autre utilisateur/-trice cyberbancaire. C'est d'autant plus valable si plusieurs personnes sont autorisées à faire des payements. Discutez avec votre banque des mesures de sécurité possibles.

> **Collaborer avec une entreprise informatique**
Si les grandes entreprises disposent souvent de leur propre service informatique, les plus petites entreprises externalisent en général ce genre de tâches. Assurez-vous que les compétences en matière de sécurité informatique soient clairement réglées entre vous et l'entreprise informatique. Cela concerne surtout les mesures techniques et organisationnelles précédemment décrites. Réglez contractuellement les responsabilités en cas de sinistre si les mesures de sécurité convenues n'ont pas été respectées.


POLICE
CRIME

4 Comment pouvez-vous contribuer à identifier les pirates?

4.1 Toute déclaration est décisive

La police n'est pas intéressée à vos secrets commerciaux et n'intervient pas dans votre infrastructure. Lors d'un piratage, elle cherche des informations et des traces permettant de clarifier le délit. L'enquête est soumise au secret de fonction. Craindre que le dépôt d'une plainte ait des répercussions négatives, telles que la mise en sûreté de vos ordinateurs durant une longue période ou la publication de votre cas, est injustifié. La police vous prend très au sérieux et en général convient d'abord avec vous des mesures de poursuite pénale. Dans la plupart des cas, il est possible de trouver une manière de procéder qui donne satisfaction aux deux parties.

Certes les enquêtes cybernétiques sont difficiles, notamment parce que de nombreux cas sont dus à des pirates actifs au niveau international. Mais elles peuvent également aboutir. L'expérience montre que de nombreux délits cybernétiques sont liés et ont des similitudes. C'est pourquoi chaque plainte peut livrer l'indice décisif sur les pirates.

4.2 Un incident doit être annoncé immédiatement

Un délit devrait être annoncé à la police ou au ministère public dès que possible. Plus vous attendez, plus il est probable que de précieuses traces soient effacées. De plus, toute action peut rendre des traces inutilisables, voire les effacer. N'importe quel poste de police enregistre une plainte par oral ou écrit. Sur le site en ligne Suisse-ePolice www.suisse-epolice.ch, vous trouvez le numéro de téléphone du poste de police le plus proche.

4.3 Procédure lors d'une déclaration sans plainte pénale

Dans certains cas, la firme peut renoncer à porter plainte. Dans ce cas, les autorités ont créé la possibilité pour l'entreprise lésée de leur transmettre des informations pour qu'elles puissent en prendre connaissance. Remplissez à cet effet un formulaire d'annonce de MELANI, www.melani.admin.ch. Grâce à ces informations, les autorités peuvent avoir un meilleur aperçu des menaces actuelles et des délits semblables ou identiques et réduire ainsi le nombre des cas non recensés. Ces indications ne peuvent cependant pas être utilisées pour une plainte pénale, ni dans une procédure pénale.

5 Que devez-vous faire, si cela arrive quand même?

Mesures d'urgence en cas de cyberattaque
Il peut arriver que – malgré toutes les mesures de précaution – vous soyez victime d'une cyberattaque. C'est pourquoi il est important que vous sachiez que faire dans un tel cas.

1. Isoler
   > Séparez immédiatement tous les systèmes du réseau. N'oubliez pas de désactiver le réseau sans fil (WLAN).
   > Attendez que la police ait sauvegardé les traces avant de restaurer les systèmes.

2. Contacter
   > Contactez immédiatement la police. Des spécialistes vous conseillent et vous secondent dans la manière de procéder, sauvegardent les traces et enquêtent. Vous trouvez sur www.suisse-epolice.ch le numéro de téléphone du poste de police le plus proche.
   > Des entreprises spécialisées privées vous aident à réparer votre infrastructure et le cas échéant à la restaurer.
   > Annoncez à MELANI les tentatives de piratage non abouties.


JDF LOR9 D9AA9Q3O
HJO JU9UO FOSD2A2I
E3A DWEU 70OIOPOE
WL SE2K 6KLJIJ1U
L3 J80J 4LQAODSO
3L F 3K 8J2SJSJ2
KS 3 9J 319U1 A3
HD S 0A H01DL L9
F0 6 S E9LAH SO
HE L D W07JW K1
D3 0 F FDJ J J