Prévenir les cyberdélits

Guide pour les petites et moyennes entreprises

Connaissez-vous le niveau de protection de votre entreprise?

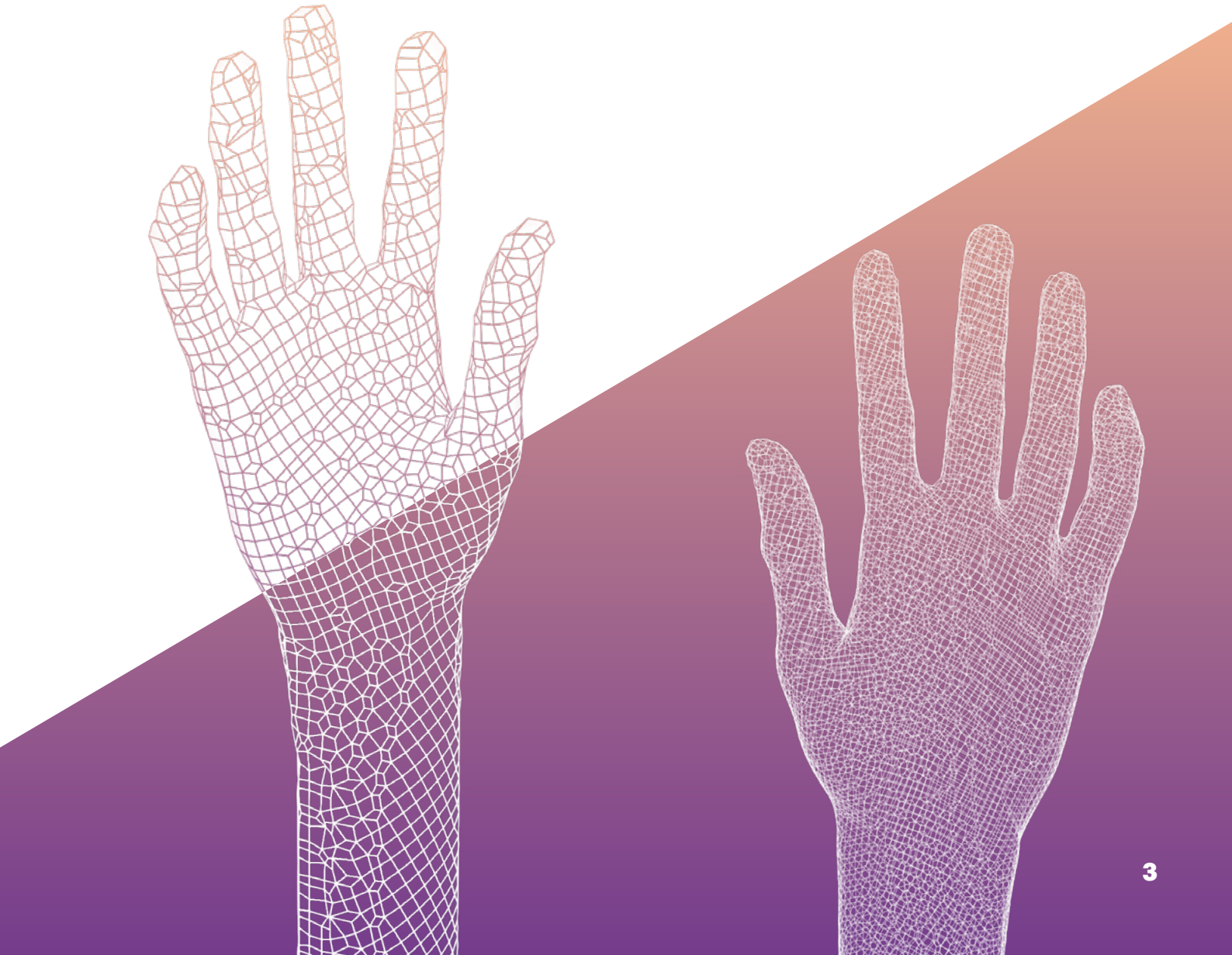
Établissez un auto-diagnostic grâce à l'aide-mémoire figurant à la fin de cette brochure.

Table des matières

1_La cybersécurité: un enjeu capital pour les entreprises

La numérisation ouvre de nouveaux horizons de croissance économique et de création d'emplois. Elle implique toutefois la mise en place de nouveaux processus et accroît la dépendance aux technologies de l'information et de la communication (TIC). Cette dépendance profite aussi aux criminels. Les cyberdélinquants emploient des techniques toujours plus élaborées pour infiltrer des réseaux, subtiliser des données ou mettre hors service des systèmes complets. De la petite entreprise artisanale à la multinationale, une cyberattaque peut représenter une menace vitale pour tout type d'entreprise.

Le présent guide de la police fournit aux cadres des petites et moyennes entreprises des recommandations pratiques pour se prémunir contre la cybercriminalité. Ces recommandations reposent en particulier sur les leçons tirées des enquêtes policières. Ce guide détaille également les étapes à suivre en cas d'attaque et expose les raisons pour lesquelles il est judicieux de signaler tout incident à la police.



2_Méthodes utilisées par les criminels

Les criminels commencent généralement par collecter des informations sur l'entreprise. En exploitant les données disponibles sur son propre site Internet de l'entreprise ou les réseaux sociaux, ils détectent les vulnérabilités dans ses systèmes, repèrent des accès potentiels au réseau et conçoivent un plan d'attaque sur mesure.

2.1 Moyens d'accès courants

Manipulation

Les criminels tirent parti de la serviabilité, de la crédulité ou d'incertitudes des collaborateurs et des collaboratrices pour leur soutirer des informations sensibles sur la sécurité ou pour infiltrer les réseaux de l'entreprise (ingénierie sociale ou «social engineering»). Les délinquants contactent leurs cibles par courriel («phishing») ou téléphone dans le but de les amener à divulguer des données sensibles. Les criminels peuvent introduire des logiciels malveillants dans des systèmes en envoyant des pièces jointes infectées ou des liens vers des sites Internet compromis, leur permettant ainsi d'infiltrer les réseaux de l'entreprise.

Le «spear phishing» est une technique de manipulation particulièrement insidieuse et répandue. L'on fait croire à des victimes ciblées qu'elles interagissent avec des personnes, des organisations ou des entreprises de confiance. Puisque la source des messages paraît fiable et que les informations sont crédibles, il peut arriver que même des individus vigilants ne détectent pas la supercherie.

Accès à distance («Remote Access»)

L'accès à distance, qui sert notamment au télétravail ou à la maintenance effectuée par des équipes de support, permet de se connecter de l'extérieur à un ordinateur ou au réseau d'une entreprise. Les criminels l'exploitent eux aussi afin de les infiltrer. Cela se produit surtout lorsque les mesures de protection de l'accès à distance sont insuffisantes.

Vulnérabilités dans les applications

L'exploitation de vulnérabilités dans les applications est aussi une méthode fréquemment utilisée lors de cyberattaques. Il peut s'agir de failles de sécurité dans les logiciels, de lacunes dans leur conception ou de configurations de sécurité défaillantes, comme l'utilisation de mots de passe peu robustes.

Pour plus d'informations sur les menaces cybernétiques actuelles, consultez le site

www.ncsc.admin.ch

2.2 Différents scénarios d'attaque

Cryptage, vol ou corruption de données.

Lors d'une attaque, les données peuvent être chiffrées et seulement débloquées contre une rançon («ransomware»), être dérobées et vendues à profit, par exemple sur le Darknet (fuite de données), ou encore servir à faire chanter l'entreprise visée. L'accès illégitime à un système informatique peut aussi avoir pour objectif la destruction de données, parfois dans le dessein de nuire à des concurrents ou de saboter une opération commerciale en cours. Dans ces situations, les attaques peuvent survenir tant de sources externes qu'internes: Les collaborateurs et collaboratrices peuvent aussi divulguer des informations confidentielles de l'entreprise à des tiers non autorisés, les détruire ou les altérer.

Arnaque au président

L'arnaque au président («CEO fraud») implique habituellement une attaque ciblée, précédée par la collecte d'informations sur l'entreprise. L'escroquerie se fait souvent par courriel falsifié de la direction de l'entreprise ou de dirigeants d'associations au service financier ou à des personnes ayant une fonction de caissier. Un récit convaincant est conçu pour persuader la victime d'effectuer des paiements prétendument urgents.

Piratage d'une messagerie professionnelle

Dans les cas de fraude à la facturation ou de piratage de la messagerie professionnelle («business e-mail compromise»), l'escroc renvoie des factures déjà émises en y ajoutant un numéro de compte bancaire (IBAN) modifié, ou il instruit les victimes de virer les paiements à venir vers un nouveau compte bénéficiaire. Le message se réfère à une correspondance électronique préexistante qui inclut un ordre de paiement ou une facture. Cela implique que les criminels aient au préalable obtenu l'accès soit au compte de messagerie de l'expéditeur, soit à celui du destinataire.

Attaque DDoS

Lors d'une attaque par déni de service distribué («Distributed Denial of Service» ou «DDoS»), les systèmes ou réseaux d'une entreprise sont complètement surchargés, les rendant temporairement inaccessibles. L'attaque se poursuit jusqu'au paiement de la rançon exigée. En cas d'attaque DDoS, les entreprises touchées, notamment celles disposant d'une boutique en ligne, peuvent subir des pertes significatives de revenus ou de commandes. Pour lancer ce type d'attaque, il n'est pas nécessaire d'avoir accédé au préalable au réseau de la victime.

Sabotage matériel

L'infrastructure TIC physique d'une entreprise peut aussi être ciblée, par exemple par le sabotage de lignes de données ou la manipulation d'équipements et de supports numériques.

3_Comment protéger votre entreprise

La protection contre la cybercriminalité devrait faire partie d'un concept global de sécurité, axé à la fois sur les aspects technologiques et organisationnels.

3.1 Définissez les responsabilités

Attribuez clairement les rôles et responsabilités en matière de cybersécurité.
En cas d'externalisation de vos TIC, formalisez les attributions de compétences par contrat. Toutefois, la responsabilité finale de la cybersécurité incombe toujours à votre entreprise.
Il est essentiel que les collaborateurs et collaboratrices sachent vers qui se tourner en cas de questions sur la sécurité informatique, comme lors de la réception d'un courriel suspect, ou qui doit être averti en cas d'incident.

3.2 Réglementez l'accès aux systèmes

Permissions et règles

Identifiez et catégorisez les données jugées sensibles au sein de votre entreprise. Mettez en place un plan de protection dédié pour ces données sensibles. Cela inclut la définition des droits d'utilisation et d'accès aux données et aux systèmes, ainsi que l'encadrement de l'usage des dispositifs personnels à des fins professionnelles.

Les collaborateurs et les collaboratrices ne doivent pas disposer de droits d'administrateur. Attribuez aux collaborateurs et aux collaboratrices uniquement les droits nécessaires à l'accomplissement de leurs tâches (principe du besoin de connaître ou du «need-to-know»). Restreignez les permissions système pour empêcher les collaborateurs et les collaboratrices d'installer ou de mettre à jour des logiciels de leur propre chef.
Pour effectuer des tâches d'administration, les administrateurs doivent utiliser un compte admin spécifique, distinct de leur compte utilisateur personnel.

Mettez en place des directives contraignantes pour les mots de passe, en exigeant qu'ils soient longs et complexes, et veillez à ce que les collaborateurs et les collaboratrices les respectent rigoureusement. Mettez en œuvre une authentification à plusieurs facteurs pour les connexions au réseau de l'entreprise. Ce point est particulièrement crucial pour les comptes admin et pour tout autre compte disposant de privilèges étendus.

Soyez prudent(e) quant aux informations que vous publiez sur le site de l'entreprise ou sur les médias sociaux, même celles qui semblent anodines: elles peuvent être recueillies par des criminels pour orchestrer des attaques sur mesure.

Comment choisir un mot de passe robuste

Un mot de passe sécurisé:

Doit comporter au moins douze caractères et inclure une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux;

Doit être aléatoire, ne figurer dans aucun dictionnaire et exclure toute donnée personnelle;

Ne doit être utilisé que pour une seule application. Ainsi, en cas de compromission d'un mot de passe, seul un compte sera affecté. Un gestionnaire de mots de passe facilite la gestion de vos divers identifiants pour les multiples applications;

Doit être renforcé par l'utilisation d'une authentification à deux facteurs.

Respectez ces règles. Le changement périodique des mots de passe n'est pas nécessaire. Les mots de passe doivent en revanche être changés s'ils ont pu être divulgués à des tiers ou si des collaborateurs ou des collaboratrices quittent votre entreprise.

Infrastructure informatique protégée et documentée

Il convient de sécuriser l'infrastructure réseau, les équipements informatiques fixes et mobiles, ainsi que le matériel spécialisé contre tout accès non autorisé, la perte, le vol ou la destruction. Tenez compte des questions de sécurité dès le processus d'achat du matériel informatique. Il convient de prendre en compte les facteurs de sécurité dès la mise en service et tout au long du cycle de vie d'un système, y compris pour son entretien et sa mise au rebut. Renseignez-vous, par exemple, sur la période pendant laquelle des mises à jour de sécurité seront disponibles pour vos équipements.
Documentez intégralement votre réseau informatique. Identifiez, répertoriez et évaluez la criticité des données, des individus, des appareils, des systèmes et des infrastructures de votre entreprise. C'est le seul moyen de savoir ce que vous devez protéger. Même en cas d'externalisation de vos technologies de l'information et de la communication, il convient d'en conserver une vision globale: c'est vous qui en assumez la responsabilité.

Sécurité de l'e-banking

Définissez clairement l'ensemble des procédures relatives aux opérations de paiement. Veillez à une application stricte de ces procédures. Par exemple, utilisez le principe de la double vérification, exigez des signatures collectives, et en cas de demandes telles que les changements de compte, utilisez un second canal de vérification (comme un appel téléphonique en complément d'un courriel reçu).
Dans la mesure du possible, optez pour un ordinateur dédié uniquement aux opérations bancaires, sans navigation Internet ou réception de courriels, tout en le maintenant à jour. Il est aussi possible de réaliser des transactions en ligne dans un environnement isolé des autres applications («sandboxing») ou via un système virtuel spécifiquement sécurisé. Abordez ces mesures de sécurité avec votre banque et informez-vous sur les éventuelles autres protections offertes.

Chiffrement des communications

Les informations confidentielles doivent être stockées sous forme chiffrée (y compris dans le cloud), et transmises à des tiers par des moyens sécurisés ou par courrier postal. L'accès aux données, notamment par des collaborateurs et des collaboratrices se connectant au réseau d'entreprise en externe, doit être sécurisé via un canal protégé comme un réseau privé virtuel (VPN). Veillez aussi à la sécurité de vos échanges avec vos clients et partenaires commerciaux. Assurez-vous tout d'abord de signer numériquement les courriels sortants. Cela confirme l'intégrité des messages et certifie leur origine. Grâce à la signature numérique des courriels, les clients peuvent à leur tour chiffrer leurs réponses. Il est aussi possible de recourir à des certificats de chiffrement pour sécuriser vos communications par courriel.

L'usage de points d'accès publics («hotspots») doit faire l'objet d'une réglementation spécifique, car ces réseaux ne sont généralement pas chiffrés et représentent une menace pour la sécurité des données.

Services cloud

Pour les services cloud, comme pour tout partenariat commercial, il convient de respecter les principes suivants: Lors de la sélection d'un fournisseur de services cloud, assurez-vous de la fiabilité de l'entreprise, par exemple en vérifiant ses certifications, la localisation de ses données, ses rapports d'activité et ses protocoles de tests. Établissez une relation de confiance et définissez clairement vos besoins et vos responsabilités respectives. Avant de recourir à un service cloud, lisez attentivement les conditions générales du fournisseur, en portant une attention particulière aux clauses de protection des données.

Considérez attentivement quelles données vous envisagez de stocker dans le cloud et évaluez les risques liés à leur sauvegarde externe. Certaines prescriptions légales spécifiques peuvent imposer un stockage des données en Suisse. Il est conseillé de ne pas stocker des données sensibles dans le cloud, ou de le faire uniquement si elles sont chiffrées. Dans ce contexte, examinez également avec attention si et comment vous souhaitez partager vos données, par exemple de manière limitée ou temporaire, et évaluez la facilité avec laquelle vous pourriez récupérer vos données du cloud pour les transférer ailleurs à l'avenir.

Gardez à l'esprit que le cloud est un support de stockage en ligne et qu'il peut donc aussi être la cible d'une cyberattaque. Les services cloud n'offrent qu'une protection partielle contre les attaques par des logiciels de rançon («ransomware»). Si vos données sont exclusivement stockées dans le cloud, elles peuvent également être chiffrées par les attaquants en cas d'incursion malveillante. La sécurité repose essentiellement sur la capacité des services à restaurer des versions antérieures des fichiers et sur la protection renforcée de cet accès, notamment par l'utilisation de mots de passe robustes et de l'authentification à deux facteurs.

Préposé fédéral à la protection des données et à la transparence,

www.edoeb.admin.ch

Office fédéral allemand de la sécurité des technologies de l'information

www.bsi.bund.de

Privatim, Conférence des Préposé(e)s suisses à la protection des données,

www.privatim.ch

Agence de l'Union européenne pour la cybersécurité,

www.enisa.europa.eu

3.3 Restez à la pointe de la technologie

Réglages de sécurité de base

Installez un logiciel antivirus sur chaque ordinateur et activez la protection en temps réel. Veillez à ce qu'il soit actualisé régulièrement et qu'il effectue un examen complet du système chaque jour.

Un vieux logiciel est une porte d'entrée prisée par les programmes malveillants. Assurez-vous que vos systèmes soient régulièrement mis à jour (déploiement des «updates»). Cela vaut pour vos programmes et applications, ainsi que pour le système de gestion de contenu (Content Management System, CMS) de vos pages Internet.

Vous devriez doter chaque ordinateur d'un pare-feu personnel. Installez le également pour protéger le réseau entrepreneurial contre les incursions venant d'Internet. Par défaut, il devrait bloquer l'ensemble des transferts, sauf s'ils sont autorisés par des règles.

Gestion des vulnérabilités

Assurez-vous de détecter rapidement les anomalies et les événements importants en matière de sécurité. Surveillez votre infrastructure réseau en utilisant des outils tels qu'un système de détection d'attaques (IDS) et un système de prévention contre les attaques (IPS). Certains d'entre eux sont également inclus dans les services de proxy web.

Définissez quels fichiers journaux (fichiers journaux des événements) sont sauvegardés et pendant combien de temps. Leur analyse fournit des informations sur la stabilité et la disponibilité des réseaux, des systèmes et des applications. De tels fichiers aident en outre à identifier l'origine d'une attaque, à obtenir des informations sur les systèmes infectés au sein de son propre réseau et à mettre en place des contre-mesures appropriées. Les aspects relevant du droit de la protection des données doivent impérativement être pris en compte dans le cadre de l'enregistrement et de l'analyse des fichiers journaux.

Astuce: Simple et complet

De nombreux systèmes d'exploitation récents intègrent déjà diverses fonctionnalités de sécurité, telles que le pare-feu, la protection du réseau, la protection contre les virus et les menaces ou les mises à jour automatiques. Activez ces fonctionnalités pour tous les appareils de votre réseau.

Les solutions «tout-en-un» proposent par exemple des systèmes de gestion unifiée des menaces. Une telle solution de sécurité complète est disponible sous forme de solution matérielle, logicielle ou cloud.

Sécurité Internet plus étendue

Pour renforcer la sécurité Internet, envisagez l'utilisation d'autres composants de sécurité, tels qu'un filtrage DNS (Domain Name System) et un proxy web. Ces outils peuvent bloquer l'accès à des sites Internet nuisibles connus ou autoriser uniquement l'accès à des sites figurant sur une liste blanche considérés comme sûrs («whitelist»). Ainsi, les demandes relatives à des sites Internet criminels sont bloquées et la sphère privée de votre entreprise est protégée.

Avant de télécharger un programme sur Internet, assurez-vous de la fiabilité du fournisseur et de la légitimité du logiciel en question. Les valeurs de hash et les signatures du logiciel doivent être vérifiées conformément aux indications du fabricant. Téléchargez les logiciels uniquement depuis le site Internet du fabricant.

Segmentation du réseau

Segmentez votre réseau d'entreprise en plusieurs domaines («segmentation du reseau»), par exemple en prévoyant des réseaux séparés pour la production, le personnel, la comptabilité, etc. Vous éviterez ainsi par exemple que l'ordinateur de commande d'installations de production qui ne peuvent plus être mises à jour serve de porte d'entrée à des attaquants et mettent en danger l'ensemble de votre réseau.
Utilisez également un service d'annuaire séparé pour vos sauvegardes (backups). Cela peut empêcher que des criminels qui se trouvent déjà dans votre système aient accès à vos sauvegardes.

Accès à distance («Remote Access»)

Protégez l'accès à distance à votre réseau par un nom d'utilisateur, un mot de passe et une authentification à deux facteurs. Installez une liaison sûre via un réseau privé virtuel (VPN), y compris pour l'accès des administrateurs et des prestataires externes de services informatiques. Il est conseillé de n'ouvrir les accès à distance pour la maintenance que lorsque cela s'avère nécessaire.

Pièces jointes et macros dangereuses

Les logiciels malveillants atterrissent sur votre ordinateur souvent à travers des pièces jointes, camouflées en pseudo-factures ou en dossiers de candidature. Les pièces jointes potentiellement dangereuses doivent donc être bloquées en amont, que ce soit au niveau de votre passerelle de messagerie ou de votre filtre anti-spam.
Vous trouverez une liste détaillée et actualisée de telles pièces jointes sur le site de l'OFCS, https://www.ncsc.admin.ch/govcert#1737483390.

Désactivez les macros Office si vous ne les utilisez pas. Assurez-vous qu'aucune macro d'origine incertaine ne puisse s'exécuter dans les documents Office. Sensibilisez vos collaborateurs et vos collaboratrices pour qu'ils/elles n'ignorent pas les avertissements y relatifs dans les programmes Office.

Astuce: Mon appareil est-il infecté par un maliciel?

Avez-vous des doutes quant au fait d'avoir téléchargé un logiciel malveillant ou quant à la présence de criminels sur votre appareil? Portez une attention particulière aux signaux d'avertissement suivants:

- Vous recevez des notifications, des images ou des signaux sonores inattendus;
- Votre programme antivirus signale un danger;
- Des programmes s'ouvrent ou établissent une connexion Internet de manière autonome;
- Des fichiers disparaissent ou sont modifiés;
- Des messages sont envoyés à des personnes de votre entourage depuis votre compte;
- Des messages sans expéditeur ni objet se trouvent dans votre boîte de messagerie;
- Votre ordinateur est allumé, mais le système d'exploitation ne se charge pas, est lent et/ou se bloque;
- Le navigateur se bloque ou vous paraît étrange.

Signalez immédiatement tout soupçon à votre spécialiste en TIC et faites contrôler votre appareil.

3.4 Sauvegardez vos données

Assurez-vous que des sauvegardes (backups) de vos informations soient effectuées régulièrement, gérées et testées (vérifier que les sauvegardes puissent être récupérées au besoin). Conservez une copie supplémentaire de vos sauvegardes hors ligne, par exemple sur un disque dur externe, et hors murs. Cela permet notamment de s'assurer qu'une copie de sauvegarde fonctionnelle est disponible en cas d'attaque par rançongiciel et de chiffrement des données en résultant.

Astuce: Enregistrez un contact de sécurité sur votre site Internet

En cas de problème de cybersécurité, il est crucial que les autorités de poursuite pénale ou les prestataires de services de sécurité puissent prendre rapidement contact avec le responsable de la sécurité compétent. La norme «security.txt» sert à indiquer de manière uniforme, sur votre site Internet, le responsable de la sécurité, ce qui permet de prendre contact avec lui plus rapidement. Vous trouverez un guide à ce sujet sur le site Internet du Centre national pour la cybersécurité:

https://www.ncsc.admin.ch/23-stxt-fr

3.5 Préparez-vous à une éventuelle attaque

Élaborez une stratégie de gestion des risques. Définissez les priorités, les restrictions et les risques maximaux acceptables pour votre organisation. Anticipez le fait qu'après un incident, vous pourriez ne pas être en mesure de fournir certains services pendant plusieurs jours, ou que vos installations de production pourraient être paralysées. Des processus bien rodés et des voies de recours à la hiérarchie sont donc indispensables pour garder le contrôle en cas d'incident. Élaborez une stratégie d'intervention en cas d'attaque et effectuez des exercices d'urgence. Mettez en place une procédure de gestion de crise appropriée. Il est également recommandé de définir en amont un concept de communication publique.

La collaboration avec des entreprises partenaires devrait également être prise en compte dans vos considérations en matière de sécurité. La réaction en chaîne qui peut être déclenchée par une attaque réussie contre une entreprise partenaire est susceptible de mettre en danger toute la chaîne de création de valeur et, par conséquent, votre entreprise même.

Les collaborateurs et collaboratrices doivent être sensibilisé(e)s aux signes potentiels d'un incident et savoir à qui signaler toute constatation à ce sujet.

Vous trouverez de plus amples informations sur la gestion stratégique et opérationnelle des risques sur le portail PME de la Confédération: https://www.kmu.admin.ch/. L'Office fédéral de la protection de la population a élaboré un guide pour la protection des infrastructures critiques: https://www.babs.admin.ch/fr/aufgabenbabs/ski/leitfaden.html. Les normes et standards courants du domaine de la gestion des risques, des situations d'urgence, des crises et de la continuité des activités constituent le fondement de ce guide. Les conséquences des cyberrisques y sont prises en compte. Ce guide peut également aider les entreprises qui ne sont pas considérées comme des infrastructures critiques à élaborer une stratégie de gestion des risques.

3.6 Restez informé(e)

Informez-vous régulièrement sur les stratégies actuelles des cybercriminels et découvrez les mesures de protection correspondantes. Les sites suivants vous permettent de rester au courant:

Police cantonale bernoise

www.police.be.ch/cyber

Office fédéral de la cybersécurité (OFCS)

www.ncsc.admin.ch

Cybercrimepolice

www.cybercrimepolice.ch

iBarry

www.ibarry.ch

Card Security

www.card-security.ch

Prévention Suisse de la Criminalité (PSC)

www.skppsc.ch

Veillez à ce que vos collaborateurs et collaboratrices reçoivent une formation régulière, adaptée à leur fonction, couvrant tous les aspects de la cybersécurité. Ne négligez en aucun cas les stagiaires, les apprenti(e)s et les collaborateurs et collaboratrices à temps partiel. Expliquez la nécessité des mesures de sécurité et l'application correcte des directives définies (p. ex. transmission d'informations ou règles relatives aux mots de passe).

Astuce: Conseils à l'attention de vos collaborateurs et collaboratrices

Ne cliquez pas sur les annexes ou liens dans les messages suspects (courriels, SMS, application de messagerie).

Évitez de transmettre des informations ou des données confidentielles via des canaux non sécurisés ou à des inconnus. Ne donnez pas non plus accès à votre ordinateur à qui que ce soit.

De manière générale, les connexions Internet publiques (y compris protégées par un mot de passe) ne sont pas sûres. Ne transmettez des informations confidentielles que par le biais de connexions qui sont également protégées par un réseau privé virtuel (VPN). Vous pouvez également utiliser une transmission de données 3G/4G/5G en itinérance pour accéder à Internet.

Ne laissez jamais votre matériel, vos documents ou vos appareils sans surveillance.

Éteignez votre ordinateur après toute intervention réalisée par des spécialistes en TIC. Dans le cas contraire, le compte admin reste actif.

Utilisez des mots de passe sûrs, générés au hasard, contenant au moins douze caractères, des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Très important: un mot de passe différent doit être utilisé pour chaque application! Complétez votre mot de passe par une authentification à deux facteurs (p. ex. code envoyé par SMS).

4_À quoi veiller en cas d'externalisation des prestations informatiques?

Veuillez trouver ci-après quelques conseils au cas où vous externalisez votre infrastructure informatique et en confiez la gestion à une ou plusieurs entreprises externes. Veuillez cependant noter que la responsabilité ne peut être ni externalisée, ni déléguée. En cas d'incident, votre entreprise peut se retrouver en bout de chaîne de responsabilités.

Exigences minimales

Vous devez contrôler la sécurité des systèmes informatiques intégrés dès leur réception. Lorsque vous avez recours à des prestations informatiques, renseignez-vous sur les conditions générales (CG) et directives applicables. Ces directives devraient faire partie intégrante des relations contractuelles entre vous et vos prestataires informatiques externes. Il est impératif de définir contractuellement les obligations de confidentialité pour les tiers en charge de la maintenance et de la gestion de vos systèmes informatiques. Ces derniers ne doivent pas accéder à des données sensibles qui ne sont pas nécessaires à leur travail. Il convient également de procéder à une analyse de la situation et de convenir d'un cadre contractuel avec chaque entreprise qui stocke des données (comme les entreprises de services cloud).

N'hésitez pas à poser des questions personnelles si quelque chose vous semble inhabituel, même si vous connaissez l'expéditeur! Ne composez jamais un numéro de téléphone figurant dans un message suspect. Cherchez les coordonnées sur le site Internet officiel en saisissant vous-même l'adresse originale dans le navigateur. Faites également attention au bouton «Répondre»: il est préférable de saisir à nouveau l'adresse électronique plutôt que de cliquer directement sur ce bouton.

Signalez les incidents suspects à votre spécialiste en TIC.

Audits de sécurité

Il convient de contrôler régulièrement que les prestations définies dans le contrat sont effectuées au moyen d'un référentiel d'audit reconnu, par exemple sur la base de COBIT (Control Objectives for Information and Related Technology) de l'ISACA (Information Systems Audit and Control Association). Ayez recours aux services d'organes de contrôle indépendants. Le prestataire informatique peut également obtenir une attestation ISAE 3402 Type 2 (International Standard on Assurance Engagements), également connue comme rapport SOC 2 (Service Organization Control). L'organe de contrôle évalue la sécurité, la disponibilité, l'intégrité et la confidentialité.

Qualifications

Des certifications selon des normes reconnues de protection des données et de sécurité de l'information ou des rapports de contrôle de tiers indépendants peuvent être utiles pour choisir un prestataire. Vous n'êtes pas obligé(e) de choisir un partenaire certifié. Mais il est recommandé que les prestataires informatiques puissent montrer qu'ils remplissent les exigences que vous posez et qu'ils peuvent assurer la disponibilité et la sécurité requises. Faites analyser ou confirmer ces conditions par un service indépendant.

Il existe un grand nombre de normes et de guides différents. Les prestataires informatiques devraient bien connaître les normes ISO 27001, ISO 22301, ISO 9001, ISO 14001 et NIST et s'y conformer. Si d'autres normes sont utilisées, l'entreprise doit en prouver la conformité (Compliance Mapping). En cas de besoin de protection accru, vous devez formuler vos propres exigences.

5_Gérer les cyberattaques

Si vous vous faites attaquer, vous devez agir rapidement. Procédez comme suit:

Isoler
Coupez immédiatement le système infecté du réseau, ce qui veut dire: tirer la prise réseau des appareils concernés et éteindre l'adaptateur Wi-Fi.

Contacter

Contactez votre partenaire TIC.

Contactez la police locale compétente. Si vous êtes en situation de détresse, composez le numéro d'urgence 112.

Convenez des étapes suivantes avec la police. Si possible, ne réinstallez pas les appareils et systèmes concernés avant que la police n'ait relevé les traces numériques cruciales.

Informez vos partenaires commerciaux et vos clients de l'incident, car ils pourraient également en être affectés.

Veillez aux devoirs d'annonce, notamment en matière de protection des données.

Gérer
Appliquez votre concept de gestion de crise. Contactez la cellule de crise et confiez la communication aux spécialistes.

5.1 Déclarez l'incident – avec ou sans dommage

Incidents avec dommages

Lors d'une attaque contre des systèmes informatiques, plusieurs infractions sont généralement commises, telles que le vol de données, l'intrusion dans un système informatique, l'escroquerie ou le chantage. Dans un tel cas, contactez la police ou le ministère public et déposez plainte.

Incidents sans dommage

Annoncez en ligne les cyberattaques avortées ou les tentatives d'escroquerie sans dommage auprès du OFCS (report.ncsc.admin.ch). Chaque annonce contribue à surveiller les activités des criminels sur Internet et à réagir en temps opportun face aux vagues d'attaques. Les informations informelles fournies au OFCS ne peuvent toutefois pas être utilisées dans le cadre d'une plainte ou d'une procédure judiciaire.

5.2 Raisons d'alerter la police

La police est consciente du caractère délicat et stressant qu'une telle situation revêt pour les entreprises. C'est pourquoi elle s'efforce d'agir de manière discrète et rapide. L'enquête est confidentielle en vertu du secret professionnel. La police n'intervient pas dans votre infrastructure, et les opérations en cours ne sont pas perturbées. En cas d'attaque, le travail de la police consiste à chercher des informations et des traces pertinentes pour élucider l'infraction. Pendant l'enquête, vous obtenez des informations importantes qui vous aident à gérer plus rapidement l'incident ou à mettre fin à la fuite d'informations cruciales concernant l'entreprise. Vous apprenez en outre comment l'auteur a procédé et où se trouvait la faille de sécurité. En cas de demande de rançon, vous bénéficiez d'un soutien professionnel. Les mesures de poursuites judiciaires sont convenues avec vous – vous pouvez en tout temps faire appel à votre conseiller juridique.

En contrepartie, vous pouvez également fournir à la police des informations pour la protection d'autres entreprises: les résultats anonymisés des procédures pénales servent à optimiser les stratégies de prévention et de lutte existantes, ainsi qu'à développer de nouvelles stratégies.

6_Sollicitez un soutien

Divers services fournissent des informations pertinentes en matière de sécurité informatique, d'aide et/ou de soutien:

Corps de police cantonaux et municipaux

Divers corps de police suisses proposent des informations spécialisées en matière de prévention de la cybercriminalité. En cas d'intérêt, veuillez vous adresser au service spécialisé du corps de police compétent à raison du lieu.

Office fédéral de la cybersécurité (OFCS)

L'OFCS, www.ncsc.ch, est le centre de compétence de la Confédération en matière de cybersécurité et donc le premier point de contact pour l'économie, l'administration, les établissements d'enseignement et la population en ce qui concerne les questions cybernétiques. Si votre entreprise fait partie des infrastructures critiques, mais n'est pas encore membre du OFCS, contactez outreach@ncsc.ch.

Office fédéral pour l'approvisionnement économique du pays (OFAE)

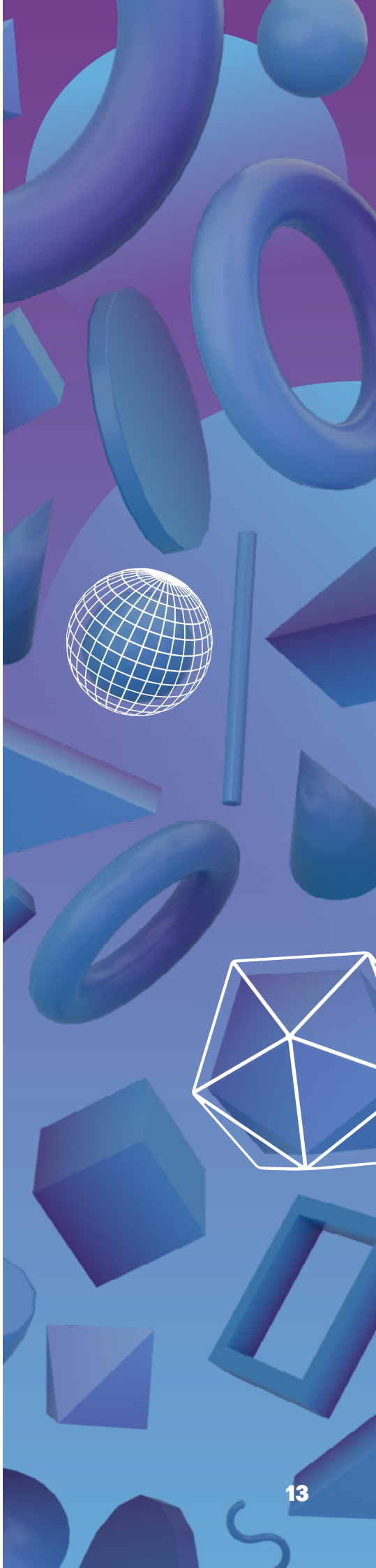
L'OFAE a élaboré une normale minimale pour les TIC ainsi qu'un outil d'évaluation. Il est recommandé aux exploitants d'infrastructures critiques d'appliquer la norme minimale pour les TIC. Toutefois, ces normes fournissent en principe une assistance et des instructions concrètes à toute entreprise ou organisation souhaitant renforcer sa résilience en matière de TIC. L'outil d'évaluation vous permet d'évaluer l'état d'avancement des mesures de protection ou de les faire contrôler par des entreprises externes (audit). Vous les trouverez sous: www.bwl.admin.ch.

Service de renseignement de la Confédération (SRC)

En collaboration avec les services de renseignement cantonaux, le SRC contribue à informer, sensibiliser et conseiller les entreprises, les hautes écoles et les instituts de recherche en matière de prolifération et d'espionnage (www.ndb.admin.ch ou prophylax@ndb.admin.ch). Une brochure abordant ce sujet et contenant des recommandations en matière de protection correspondantes est disponible sur le site Internet du SRC.

Protection des données

Depuis le 1er septembre 2023, la Suisse dispose d'une nouvelle loi sur la protection des données de la population. En tant qu'entreprise, vous devez adapter votre traitement de données personnelles à ces dispositions. Le traitement des données personnelles par des personnes privées et par des organes fédéraux relève de la compétence du Préposé fédéral à la protection des données et à la transparence (PFPDT), www.edoeb.admin.ch. Vous trouverez des informations sur la protection des données sur le portail PME de la Confédération www.kmu.admin.ch.
Des outils de protection des données et une liste des autorités de surveillance en la matière sont publiés sur le site Internet de privatim, la Conférence des Préposé(e)s suisses à la protection des données www.privatim.ch.



7_Annexes

7.1 Aide-mémoire: évaluation rapide de votre cybersécurité

Cet aide-mémoire vous aide à approfondir les questions les plus importantes en matière de cybersécurité. Un «je ne sais pas» ou un «non» signifie que vous devriez clarifier la question.
Au cas où vous avez externalisé votre infrastructure informatique, vérifiez que les points suivants soient couverts par le contrat avec votre prestataire informatique.

Remplissez également cette évaluation de la cybersécurité relativement à d'éventuelles filiales et aux fournisseurs clés de l'entreprise. Les échanges avec les principales entreprises partenaires sont également recommandés, car les cyberincidents peuvent avoir des répercussions sur l'ensemble de la chaîne de création de valeur.

Sur le site Internet de l'Office fédéral pour l'approvisionnement économique du pays www.bwl.admin.ch, vous trouverez un outil d'évaluation détaillée de la norme minimale pour les TIC. Vous pouvez ainsi évaluer l'état d'avancement des mesures de protection ou les faire contrôler par des entreprises externes (audit).

Vérifiez régulièrement les points figurant dans l'aide-mémoire. En effet, il convient d'assurer la cybersécurité en permanence.

Organisation et processus	Oui	Non	Ne sais pas
Votre entreprise a-t-elle défini qui est responsable de la cybersécurité?	☐	☐	☐
Avez-vous déjà effectué des évaluations des cyberrisques?	☐	☐	☐
Les principaux cyberrisques ont-ils été identifiés, sont-ils surveillés et ont-ils été documentés?	☐	☐	☐
Savez-vous à quoi ressemble votre paysage informatique (p. ex. inventaire, logiciels, systèmes informatiques externes pertinents)?	☐	☐	☐
Disposez-vous d'un plan d'urgence ainsi que d'une stratégie de communication en cas de cyberattaque?	☐	☐	☐
L'accès physique aux infrastructures d'ordinateurs, serveurs et réseau ainsi qu'aux lignes de données est-il protégé contre l'accès de tiers?	☐	☐	☐
Sensibilisation des collaborateurs et collaboratrices			
Les collaborateurs et collaboratrices sont-ils/elles régulièrement formé(e)s à la cybersécurité?	☐	☐	☐
La direction et les collaborateurs et les collaboratrices ayant compétence en matière de transfert de données sensibles ou ayant accès à des données sensibles reçoivent-ils/elles des formations adaptées à leur fonction?	☐	☐	☐
Les collaborateurs et collaboratrices ont-ils/elles connaissance des directives de l'entreprise?	☐	☐	☐
Protection des données			
Existe-t-il une directive sur la protection des données/politique en matière de sécurité des informations et les collaborateurs et collaboratrices en ont-ils/elles connaissance?	☐	☐	☐
Les prescriptions en vigueur en matière de protection, de sauvegarde et de traitement des données sont-elles rigoureusement et correctement mises en œuvre?	☐	☐	☐

Contrôle des accès et droits	Oui	Non	Ne sais pas
Disposez-vous d'un concept d'autorisation et de rôle pour les collaborateurs et les collaboratrices (accès uniquement aux informations pertinentes pour la fonction)?	☐	☐	☐
Les droits d'administrateur locaux sont-ils bloqués sur les postes de travail des collaborateurs et des collaboratrices?	☐	☐	☐
Disposez-vous d'une directive relative aux mots de passe et utilisez-vous des procédures d'authentification fortes?	☐	☐	☐
Réseau protégé			
Les différents secteurs de votre entreprise, par exemple les ressources humaines et la comptabilité, sont-ils séparés (segmentation du réseau) et les accès sont-ils réglementés? Alternative pour les micro-entreprises: Utilisez-vous des ordinateurs ou des systèmes distincts pour les différents secteurs d'activité, tels que l'administration, les ressources humaines et l'e-banking?	☐	☐	☐
Dans votre entreprise, l'accès externe (accès à distance) à l'infrastructure d'ordinateurs, serveurs et réseau ainsi qu'au cloud (VPN, authentification à deux facteurs) est-il protégé et peut-il être séparé en cas de non-utilisation (contrôle d'accès)?	☐	☐	☐
Les pièces jointes considérées comme potentiellement dangereuses sont-elles définies dans le programme de courrier électronique, et l'exécution des macros est-elle réglée dans les documents Office?	☐	☐	☐
Utilisez-vous des logiciels et/ou du matériel obsolètes qui ne bénéficient officiellement plus des mises à jour de sécurité?	☐	☐	☐
Saisissez-vous en temps utile les corrections (correctifs et mises à jour critiques pour la sécurité) pour vos systèmes et logiciels informatiques?	☐	☐	☐
Utilisez-vous des antivirus, des antispyware ou une protection équivalente contre les programmes malveillants?	☐	☐	☐
Disposez-vous d'un processus pour identifier les vulnérabilités de votre logiciel ou de vos systèmes informatiques afin que des mesures puissent être prises et que les vulnérabilités puissent être traitées (p. ex. IPS, IDS, Logserver)?	☐	☐	☐
Tous les points d'accès à Internet sont-ils protégés par des pare-feu?	☐	☐	☐
Exploitez-vous des réseaux sans fil chiffrés?	☐	☐	☐
Utilisez-vous des composants de sécurité Internet étendue, tels qu'un filtrage DNS («Domain Name System») et un proxy web?	☐	☐	☐
Sauvegarde (backup)			
Des sauvegardes de données sont-elles régulièrement effectuées, gérées et testées (possibilité de récupérer les sauvegardes)?	☐	☐	☐
Une copie de la sauvegarde est-elle conservée séparément (hors ligne), et une autre copie est-elle conservée ailleurs qu'au centre de traitement de données (hors site, p. ex. sur un cloud, dans un coffre-fort à la banque)?	☐	☐	☐
Utilisez-vous un service d'annuaire séparé pour vos sauvegardes?	☐	☐	☐
Contrat avec l'entreprise de services informatiques et de services cloud			
Les responsabilités en cas de dommage et les limites à l'obligation au titre des prestations définies (p.ex. force majeure) sont-elles réglées dans le contrat?	☐	☐	☐
Les niveaux de service pour le fonctionnement normal et d'urgence sont-ils clairement formulés?	☐	☐	☐
Avez-vous prévu une stratégie de sortie? Est-elle définie dans le contrat, notamment pour les solutions cloud?	☐	☐	☐
Collaboration avec les autorités de poursuite pénale			
La personne responsable et vos interlocuteurs en cas d'incident informatique sont-ils définis et disponibles?	☐	☐	☐

7.2 Certifications, normes et guides

Il existe une multitude de normes et de certificats différents qui présentent des objectifs principaux différents. En fonction des besoins, ils peuvent être pris différemment en compte lors de la sélection. Voici quelques exemples:

Gestion de crise, continuité des activités, reprise d'activité après sinistre

ISO 22301, Systèmes de management de la continuité des activités
ISO 27031, Préparation des technologies de la communication et de l'information pour la continuité d'activité
BS 11200, Crisis management: guidance and good practice

Sécurité des données et de l'information

ISO 27001, Systèmes de management de la sécurité de l'information
ISO 27701, Extension d'ISO 27001 au management de la protection de la vie privée
ISO 30141, Architecture de référence de l'Internet des objets (IoT) – Confidentialité des données

Orientation conforme au Règlement général de l'Union Européenne 2016/679 sur la protection des données (RGPD)NIST Cyber Security Framework

Guides techniques

EN 50173, Systèmes de câblage générique
EN 50600, Installations et infrastructures de centres de traitement de données
ANSI/TIA-942, Centres de traitement de données
CEI 62443, Réseaux industriels de communication – Sécurité dans les réseaux et les systèmes

Cloud

IISO 27017, Code de bonnes pratiques pour les contrôles de sécurité de l'information (fondés sur l'ISO/IEC 27002, guide des mesures de sécurité de l'information)
ISO 27018, Code de bonnes pratiques pour la protection des informations personnelles identifiables (PII) dans l'informatique en nuage public agissant comme processeur de PII

Autres (surtout pour les fournisseurs de matériel)

ISO 9001, Systèmes de management de la qualité
ISO 14001, Systèmes de management environnemental

Guide pour mandants

ISO 22300, Sécurité et résilience — vocabulaire
ISO 22318, Continuité de la chaîne d'approvisionnement
ISO 27036, Sécurité d'information pour la relation avec le fournisseur
ISO 31010, Management du risque

Certains prestataires proposent des certifications sans accréditation. Le Service d'accréditation suisse SAS évalue et accrédite les organismes d'évaluation de la conformité (OEC).

Vous pouvez rechercher quel organisme de certification est agréé pour quelles normes: Recherche organismes accrédités SAS.

Impressum
Contenu: Police cantonale bernoise, service projets et cybercriminalité, sur mandat du réseau de soutien aux enquêtes de lutte contre la criminalité numérique (NEDIK). En collaboration avec l'Office fédéral de la cybersécurité (OFCS) et l'Office fédéral pour l'approvisionnement économique du pays (OFAE).

Conception et mise en page: NEDIK

Contact: praevention@police.be.ch, tél.: 031 638 91 00

NEDIK

POLICE

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral pour l'approvisionnement économique du pays OFAE

Office fédéral de la cybersécurité OFCS