Cybersecurity-Check pour les PME

Version 4.0, 1er décembre 2025

Les PME ciblées par des cyberattaques

Les petites et moyennes entreprises (PME) sont de plus en plus souvent la cible des cybercriminels. Selon *Netzwoche*, le nombre de cyberattaques en Suisse a augmenté de 113 % au premier trimestre 2025 par rapport à l'année précédente, une hausse alarmante. L'augmentation des attaques utilisant l'intelligence artificielle, notamment les technologies de deepfake pour commettre des fraudes visant les dirigeants, est particulièrement préoccupante (Source : *Portail PME SECO*).

Les causes les plus fréquentes des attaques réussies sont :

- Protection insuffisante des systèmes et des processus,
- Systèmes informatiques obsolètes,
- Exploitation du facteur humain (ingénierie sociale)
- Préparation insuffisante aux incidents de sécurité.

Le www.cybersecurity-check.ch a été développé pour les PME dans le cadre de la Stratégie nationale de protection de la Suisse contre les cyberrisques (SNPC), la première édition a été publiée en 2020. Cette version 4.0 entièrement révisée (à compter de novembre 2025) a été créée en collaboration avec les partenaires suivants : ASDS, OFCS, BDO, digitalswitzerland, EXPERTsuisse, Gobugfree, ISSS, SATW, SISA,

SNV, SQS, Suissedigital et SVV.

Un outil pratique pour protéger les PME

Le Cybersecurity-Check propose aux PME des recommandations concrètes et applicables pour renforcer efficacement leur sécurité. Il prend en compte l'évolution des menaces, les nouvelles technologies et les exigences légales. Sa structure modulaire et son orientation pratique le rendent facile à utiliser, même pour les personnes sans connaissances techniques.

L'autodiagnostic intégré permet aux entreprises d'évaluer et d'identifier leur niveau de sécurité actuel.

- Quelles mesures de protection techniques, organisationnelles, procédurales et relatives aux employés ont déjà été mises en œuvre,
- et lorsqu'il existe un besoin spécifique d'agir pour garantir un niveau minimal de cybersécurité.

Avis : Le Cybersecurity-Check ne remplace pas le conseil individuel en sécurité, mais offre une introduction solide et pratique aux PME.

Table des matières

1 Organisation et processus

Pourquoi est-ce important ?

Les cyberincidents peuvent toucher les entreprises de toutes tailles, y compris les PME. Ce qui est déterminant, ce n'est pas seulement la préparation aux situations d'urgence, mais aussi l'amélioration continue et la prévention grâce à un niveau de sécurité organisationnel élevé.. En établissant des processus clairs et en les vérifiant régulièrement, vous pouvez réagir rapidement en cas d'urgence, limiter les dommages et reprendre rapidement vos activités commerciales.

Un bon niveau de sécurité organisationnelle signifie :

- Des responsabilités clairement définies,
- Sauvegarde régulière des informations critiques,
- Répartition et gestion rigoureuses des droits d'accès,
- Un plan d'urgence bien pensé et testé (y compris des canaux de communication alternatifs).

Que puis-je faire ?

- ☑ Répertorier de manière exhaustive et précise le matériel informatique et les applications utilisés dans les processus critiques de l'entreprise et protégez ces actifs contre tout accès non autorisé.
- ☑ Mettre en place des sauvegardes régulières et automatisées des données critiques pour l'entreprise.
- ☑ Renforcer la gestion des utilisateurs grâce aux droits d'accès basés sur les rôles et à l'authentification à deux facteurs.
- ☑ Élaborer et tester un plan d'urgence complet qui prenne en compte les menaces actuelles (par exemple, en utilisant des modèles de plans d'urgence disponibles sur OFCS et BDO).

2 Sensibilisation et implication des employés

Pourquoi est-ce important ?

L'exploitation du facteur humain (ingénierie sociale) est un élément clé de la réussite des cyberattaques. Des employés sensibilisés repèrent plus rapidement les activités suspectes, évitent les erreurs courantes (comme cliquer sur des liens d'hameçonnage) et gardent leur sang-froid dans les situations critiques. Selon l'OFCS, l'ingénierie sociale est responsable, au moins en partie, des dommages causés dans plus de 80 % des cyberincidents survenus dans les entreprises suisses. Par conséquent, des employés informés constituent le principal atout de votre stratégie de cybersécurité.

Un bon comportement en matière de sécurité signifie :

- Reconnaître les messages et les situations suspectes,
- une gestion appropriée des mots de passe et des informations sensibles,
- des directives claires pour les utilisateurs des systèmes informatiques et des canaux de communication,des formations et des exercices réguliers.

Que puis-je faire ?

- ☑ Ancrer la sensibilisation des collaborateurs dans le quotidien de l'entreprise.Assurer la meilleure protection possible pour lesapplications grâce à des mots de passe sécurisés et à l'authentification à deux facteurs (2FA).
- ☑ Définir des consignes d'utilisation pour une utilisation sécurisée d'Internet et des courriels.

3 Mesures de protection techniques

Pourquoi est-ce important ?

Les mesures de sécurité technique constituent le fondement de toute cybersécurité. Sans systèmes actuels, mécanismes de protection et communications chiffrées, votre entreprise reste vulnérable, quel que soit le niveau de formation de votre organisation et de vos collaborateurs.

En 2025, les attaques ont été davantage automatisées, notamment grâce à des analyses de vulnérabilité basées sur l'IA, l'exploitation du cloud et des attaques via des appareils obsolètes ou non protégés (par exemple, routeurs, IoT, accès à distance). Les vulnérabilités logicielles et l'absence de mises à jour restent parmi les portes d'entrée les plus courantes pour les attaquants.Un niveau élevé de protection technique signifie :

- Des systèmes et applications mis à jour,
- l'utilisation de logiciels de sécurité,
- une communication chiffrée,
- la protection de tous les appareils connectés au réseau.

Que puis-je faire ?

- ☑ Utiliser le matériel et les logiciels appropriés (par exemple, pare-feu et logiciels antivirus) pour renforcer la sécurité.
- ☑ Veiller à mettre à jour régulièrement les logiciels et les appareils.
- ☑ Ne pas connecter d'appareils obsolètes pour lesquels aucune mise à jour logicielle n'est disponible, et ne connecter à Internet que les systèmes absolument nécessaires.

Avis : Les mesures de sécurité technique ne constituent pas un projet ponctuel, mais un processus continu. Il est essentiel de procéder à des audits réguliers, ou de faire appel à des spécialistes informatiques externes et à des prestataires certifiés pour identifier et corriger les failles de sécurité.

4 Protection des données et informations juridiques

Pourquoi est-ce important ?

La protection des données personnelles est essentielle pour instaurer la confiance avec les clients, mais constitue également une obligation légale. Les violations des lois sur la protection des données peuvent entraîner de lourdes amendes, des poursuites judiciaires et un préjudice considérable à la réputation, notamment lorsqu'elles résultent d'incidents informatiques.

Depuis l'entrée en vigueur de la loi suisse révisée sur la protection des données (LPD) en 2023 et la mise en œuvre du Règlement général sur la protection des données (RGPD) de l'UE pour les entreprises suisses ayant des liens avec l'UE, les dispositions suivantes s'appliquent : toute personne traitant des données à caractère personnel doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour en assurer la sécurité. Les responsables du traitement peuvent être tenus personnellement responsables en cas de violation de données.

Le traitement des données conformément à la loi signifie :

- La transparence du traitement des données à l'égard des personnes concernées,
- la protection contre l'accès non autorisé et la perte,
- des responsabilités et des obligations claires,
- un accord de traitement des données avec des prestataires de services externes (Modèle)
- la connaissance et le respect des obligations légales de déclaration en cas de violation de données (guide)

Que puis-je faire ?

- ☑ Veiller à ce que le traitement des données personnelles soit conforme aux exigences de la loi sur la protection des données (LPD) et, le cas échéant, du Règlement général sur la protection des données (RGPD).
- ☑ Documenter les données qui sont collectées, traitées et stockées – et dans quel but.
- ☑ Prendre des mesures techniques et organisationnelles pour protéger ces données.

Avis : La protection des données concerne tous les aspects : de l' entreprise, du site web et du CRM jusqu'aux ressources humaines. Il ne s'agit pas seulement d'une tâche informatique, mais d'une responsabilité partagée par toute l'entreprise. Vous trouverez plus d'informations et de ressources sur www.edoeb.admin.ch/fr/protection-des-donnees ou www.kmu.admin.ch.

5 Partenaires externes et prestataires de services

Pourquoi est-ce important ?

De nombreuses PME font aujourd'hui appel à des prestataires de services informatiques externes, des fournisseurs de cloud ou de solutions logicielles spécialisées. Ce choix est judicieux, car ces partenaires qualifiés apportent une expertise, une expérience et des technologies modernes souvent indisponibles en interne. Une collaboration fructueuse avec des prestataires externes est donc un élément clé d'une stratégie de cybersécurité robuste.

Parallèlement, il demeure essentiel de conclure des contrats clairs, de définir les responsabilités et de vérifier régulièrement la conformité aux normes de sécurité. Car même en cas d'externalisation de certaines tâches, la responsabilité de la sécurité des données et des systèmes incombe toujours à l'entreprise.

Une approche sécurisée des relations avec les partenaires externes signifie :

- Une sélection de prestataires de services qualifiés possédant une expertise avérée en matière de sécurité,
- des exigences de sécurité consignées par écrit,
- une communication transparente et une planification d'urgence conjointe,
- une attribution et une gestion ciblée des droits d'accès.

Que puis-je faire ?

- ☑ Travailler avec des partenaires informatiques qualifiés qui peuvent démontrer leur conformité aux normes de sécurité (CyberSeal, SN EN ISO/IEC 27001).
- ☑ Documenter par écrit les exigences techniques et organisationnelles.
- ☑ Intégrer activement les fournisseurs de services informatiques dans les processus de planification d'urgence et de sécurité.

Avis : Même si un prestataire « s'occupe de tout », vous restez responsable en tant qu'entreprise (notamment de la sauvegarde et de la restauration des données). Vérifiez régulièrement que vos partenaires respectent les mesures de sécurité adaptées à votre secteur d'activité et à la taille de votre entreprise.

Pour toute question relative au choix des prestataires ou à la rédaction des contrats, veuillez consulter les plateformes nationales telles que OFCS - Informations pour les entreprises, Alliance Sécurité Digitale Suisse - CyberSeal, ITSec4KMU ou vos associations professionnelles.

6 Tests d'intrusion et analyse de vulnérabilité

Pourquoi est-ce important ?

Même les mesures de sécurité les mieux intentionnées ne sont efficaces que si elles sont mises en œuvre. Les vulnérabilités des systèmes, des réseaux ou des applications passent souvent inaperçues

jusqu'à ce qu'elles soient exploitées par des attaquants. Il est donc crucial de tester régulièrement votre infrastructure informatique, idéalement par des tiers qualifiés et indépendants.

En particulier en 2025, alors que les attaquants utilisent de plus en plus des analyses automatisées et basées sur l'IA pour identifier précisément les vulnérabilités des entreprises, une approche proactive est cruciale. Un test d'intrusion (pentest) simule des attaques réelles – de manière contrôlée et traçable – dans le but d'identifier et de corriger les vulnérabilités au plus tôt.

Un test professionnel révèle:

- une clarté sur les vulnérabilités de sécurité réelles,
- une évaluation réaliste du risque,
- des recommandations spécifiques pour l'amélioration.

Que puis-je faire ?

- ☑ Effectuer régulièrement des analyses de vulnérabilité des systèmes, en interne ou par l'intermédiaire d'experts externes.
- ☑ Effectuer un test d'intrusion annuellement ou chaque fois que des modifications importantes sont apportées aux systèmes critiques de l'entreprise.
- ☑ Traiter systématiquement les vulnérabilités identifiées et documenter les mesures prises.

Avis : Pour les PME de plus petite taille, les analyses de vulnérabilité standardisées peuvent constituer une première étape importante. Des plateformes telles que GoBugFree ou ITSec4KMU offrent un soutien pratique. Ceux qui souhaitent aller plus loin peuvent se connecter avec des partenaires du réseau de cybersécurité (par exemple, SCD DNA, Alliance Sécurité Digitale Suisse - CyberSeall) afin d'identifier des prestataires appropriés.

Encadré : Tests d'intrusion vs. hacking éthique

Tests d'intrusion (Pentest)

Un test clairement défini, structuré et ciblé, axé sur un domaine spécifique (par exemple, une application web, un segment de réseau). Son objectif est d'identifier et d'évaluer les vulnérabilités techniques.

Hacking éthique (piratage amical)

Une approche plus large et moins rigide, fonctionnant comme un véritable attaquant, mais avec autorisation. Cela implique d'examiner les vulnérabilités techniques, organisationnelles et conceptuelles à l'échelle de l'entreprise.

Un test d'intrusion peut faire partie d'un projet de d'hacking éthique global, mais il est défini de manière beaucoup plus restrictive et standardisé sur le plan méthodologique.

7 Auto-évaluation de la cybersécurité

Votre entreprise est-elle suffisamment protégée et préparée contre les cyberattaques ? Vérifiez dès maintenant si vous répondez aux exigences minimales.

1. Organisation et processus	Oui	Non	Je ne sais pas
Les personnes de contact pour la sécurité informatique sont-elles connues (internes ou externes) ?			
La cybersécurité est-elle un sujet régulièrement abordé lors des réunions de direction ?			
La cybersécurité fait-elle partie de votre gestion des risques et est-elle abordée lors des réunions de direction ?			
Avez-vous recensé et documenté l'intégralité des ressources informatiques et des processus critiques de votre entreprise ?			
Existe-t-il des sauvegardes indépendantes du système et du fournisseur, et sont-elles restaurables ?			
Conservez-vous au moins une copie de sauvegarde dans un emplacement externe, sécurisé et hors ligne ?			
Testez-vous régulièrement la restauration de vos données à partir de sauvegardes ?			
Utilisez-vous des comptes d'utilisateurs distincts pour les tâches administrateurs et les tâches courantes ?			
Tous les utilisateurs disposent-ils uniquement des droits d'accès nécessaires à leurs tâches (principe du moindre privilège) ?			
Les droits d'accès sont-ils attribués de manière cohérente en fonction des rôles (par exemple, comptabilité, RH, informatique) ?			
Utilisez-vous uniquement des comptes utilisateurs personnels et aucun compte partagé ?			
Veillez-vous à modifier immédiatement les mots de passe des comptes d'entreprise et de groupe lorsque des employés quittent l'entreprise ?			
Désactivez-vous immédiatement les comptes utilisateurs en cas de départ ou de changement de rôle ?			
Avez-vous identifié et documenté les systèmes, les données et les informations critiques pour l'entreprise ?			
Existe-t-il des solutions de repli définies, telles que du matériel de secours ou des accords d'urgence avec les fournisseurs ?			
Existe-t-il une documentation indiquant qui travaille avec quels systèmes, y compris les coordonnées des personnes concernées ?			
Avez-vous défini des mesures immédiates en cas d'urgence, et le plan d'urgence est-il disponible hors ligne, par exemple en déconnectant les systèmes affectés du réseau ?			
Avez-vous prévu des mesures pour rétablir rapidement la capacité de travail (par exemple, imprimer les coordonnées importantes) ?			
Les rôles et les responsabilités sont-ils clairement définis dans le plan d'urgence			

(par exemple, réponse informatique, clarification juridique, communication, notification des autorités) ?			
Vous entraînez-vous régulièrement au plan d'urgence avec votre équipe ?			

2. Sensibilisation et implication des employés	Oui	Non	Je ne sais pas
Dispensez-vous une formation de base en cybersécurité à tous vos employés ?			
La formation aborde-t-elle des sujets tels que les avantages de la sécurité informatique, la gestion des identifiants de connexion, le traitement sécurisé des informations et l'utilisation sécurisée d'Internet et du courrier électronique ?			
Répétez-vous régulièrement cette formation (par exemple, annuellement) ?			
Utilisez-vous des exemples concrets comme le phishing, la fraude au PDG ou les deepfakes dans vos formations ?			
Empêchez-vous le branchement incontrôlé d'appareils tels que des téléphones portables sur les ports USB des équipements de travail ?			
Favorisez-vous une culture où les employés peuvent communiquer ouvertement et demander de l'aide en cas d'incertitude, sans chercher à blâmer qui que ce soit ?			
Rendez-vous la cybersécurité visible en interne, par exemple au moyen d'affiches, de bulletins d'information ou de courtes vidéos ?			
Vos mots de passe utilisent-ils au moins 12 caractères et incluent-ils des lettres majuscules et minuscules, des chiffres et des caractères spéciaux ?			
Utilisez-vous ou recommandez-vous des gestionnaires de mots de passe dans votre entreprise ?			
Utilisez-vous l'authentification à deux facteurs (2FA) chaque fois que cela est possible ?			
Évitez-vous de réutiliser vos mots de passe ? Vérifiez régulièrement si les mots de passe de vos employés ont été compromis (Have I Been Pwned ?).			
Avez-vous défini des directives d'utilisation claires et compréhensibles pour la messagerie électronique, Internet, les médias sociaux et les appareils mobiles ?			
Le partage des identifiants de connexion est-il expressément interdit ?			
Sensibilisez-vous vos employés aux courriels suspects (par exemple, provenant d'expéditeurs inconnus ou présentant un style inhabituel) ?			
Existe-t-il des avertissements contre l'utilisation des réseaux Wi-Fi publics et non sécurisés ?			
L'installation d'applications ou de logiciels inconnus est-elle réglementée (sur ordinateur et mobile) ?			
La direction est-elle également activement sensibilisée et joue-t-elle un rôle de modèle en matière de cybersécurité ?			

3. Mesures de protection techniques	Oui	Non	Je ne sais pas
Les mises à jour automatiques sont-elles activées pour les systèmes d'exploitation, les applications et les services cloud ?			
Vérifiez-vous régulièrement l'état des mises à jour de tous vos appareils, y compris les imprimantes, les routeurs, les appareils photo ou les smartphones ?			
Utilisez-vous des outils de gestion centralisée pour la gestion des correctifs (si cela est techniquement et opérationnellement possible) ?			
Les appareils ne pouvant pas être mis à jour sont-ils systématiquement déconnectés d'Internet ou remplacés ?			
Utilisez-vous une solution de protection des terminaux (y compris un logiciel antivirus) pour détecter et prévenir les comportements suspects ?			
Un pare-feu est-il actif et bloque-t-il les accès non autorisés ?			
Utilisez-vous des solutions de gestion des appareils mobiles (MDM) pour vos appareils mobiles, ou envisagez-vous de les utiliser ?			
Utilisez-vous des connexions chiffrées (par exemple, un VPN) pour vos courriels, les transferts de fichiers et l'accès à distance ?			
Appliquer systématiquement une authentification forte (authentification à deux facteurs (2FA), clés d'accès) pour l'accès au système externe ?			
Avez-vous segmenté votre réseau pour séparer les systèmes sensibles (par exemple, la comptabilité) de l'utilisation générale (par exemple, le Wi-Fi invité) ?			
Les interfaces inutilisées, telles que les ports USB libres ou le Bluetooth, sont-elles désactivées ?			
Les salles serveurs sont-elles physiquement sécurisées et n'existe-t-il aucune connexion réseau librement accessible dans les zones publiques ?			

4. Protection des données et informations juridiques	Oui	Non	Je ne sais pas
Tenez-vous un registre complet de toutes les données personnelles traitées au sein de l'entreprise (par exemple, les données clients, les données des employés, les données de connexion) ?			
Avez-vous documenté l'objectif de la collecte de données pour chaque type de données (par exemple, traitement des contrats, marketing, RH) ?			
Avez-vous vérifié s'il existe une base juridique valable pour chaque traitement de données (par exemple, consentement, contrat, obligation légale) ?			
Appliquez-vous les mêmes mesures de sécurité techniques aux données personnelles qu'aux autres données de votre entreprise (par exemple, contrôle d'accès, chiffrement, sauvegarde) ?			
Est-il garanti que seules les personnes autorisées peuvent accéder aux données personnelles ?			
Votre site web comporte-t-il une politique de confidentialité ?			
Donnez-vous aux personnes concernées la possibilité de demander des informations sur leurs données et d'en demander la rectification ou la suppression ?			
Votre entreprise dispose-t-elle d'une procédure définie pour gérer les incidents de protection des données (par exemple, les données clients volées) ?			
Pouvez-vous garantir que les violations de données devant être signalées le sont au PFPDT dans un délai de 72 heures ?			
Les personnes concernées sont-elles informées si leurs droits risquent d'être violés en raison d'une fuite de données ?			
Avez-vous conclu un accord écrit de traitement des données avec tous les sous-traitants (c'est-à-dire les partenaires qui traitent des données personnelles pour votre organisation) ?			
Vérifiez-vous si vos fournisseurs de services informatiques respectent les normes de sécurité appropriées (par exemple, CyberSeal) ?			

5. Partenaires externes et prestataires de services	Oui	Non	Je ne sais pas
Lors du choix de vos fournisseurs de services informatiques et de cloud, recherchez des certifications de sécurité reconnues (par exemple, ISO 27001, CyberSeal) ?			
Demandez-vous régulièrement des preuves des mesures de sécurité actuelles telles que la gestion des correctifs, les sauvegardes et les procédures d'urgence ?			
Utilisez-vous des outils comme le test rapide de cybersécurité pour PME afin de clarifier les exigences avec les fournisseurs potentiels ?			
Existe-t-il des accords écrits, notamment des accords de niveau de service (SLA), pour la coopération avec des partenaires externes, en particulier en ce qui concerne le traitement des données ou l'accès au système ?			
Avez-vous défini dans ce document les droits d'accès, les obligations de signalement en cas d'incidents de sécurité et le lieu de traitement des données (par exemple, Suisse, UE, pays tiers) ?			
Des partenaires externes sont-ils impliqués dans votre planification d'urgence (par exemple, qui est informé, quand et comment) ?			
Planifiez-vous et menez-vous des exercices ou des tests de sécurité conjoints (par exemple, en réponse à des attaques de phishing ou à des pannes de système) ?			
Recevez-vous des mises à jour régulières et proactives sur l'état de la sécurité de la part de vos fournisseurs de services ?			
Les personnes extérieures ne reçoivent-elles que les droits d'accès minimaux nécessaires (principe du moindre privilège) ?			
Documentez-vous clairement qui a accès à quels systèmes, y compris la durée et la finalité de l'accès ?			
Les droits d'accès externes sont-ils immédiatement supprimés lorsqu'ils ne sont plus nécessaires (par exemple, après l'achèvement d'un projet) ?			

Note préliminaire : Ceci s'applique particulièrement aux PME qui développent et exploitent leurs propres solutions ou qui sont directement exposées sur Internet.

6. Tests d'intrusion et analyse de vulnérabilité	Oui	Non	Je ne sais pas
Précisez-vous au préalable la portée du test (par exemple, réseau, applications Web, accès à distance, WLAN) ?			
Accordez-vous la priorité à la mise en œuvre des mesures identifiées lors des analyses de vulnérabilité et des tests d'intrusion, notamment dans les zones à haut risque ?			
Documentez-vous les mesures prises (par exemple, les mises à jour effectuées, les modifications de configuration) ?			
Effectuez-vous des tests de suivi pour vérifier que les vulnérabilités identifiées ont été entièrement résolues ?			
Existe-t-il des critères clairs concernant le moment où les analyses de vulnérabilité ou les tests d'intrusion sont effectués (par exemple, après les mises à jour, annuellement) ?			
Ces tests font-ils partie intégrante de votre stratégie de sécurité informatique ?			

8 Annexes

Liens utiles

Autorités et organismes officiels

- **Office fédéral de la cybersécurité (OFCS) – « Protégez votre PME »**
  Directives officielles, listes de contrôle et recommandations pour les PME.
  Office fédéral de la cybersécurité (OFCS) – Protégez votre PME
  Office fédéral de la cybersécurité (OFCS) – Informations pour des entreprises
- **Préposé fédéral à la protection des données et à la transparence (PFPDT)**
  Lignes directrices, modèles, FAQ, exigences légales de la loi suisse sur la protection des données (LPD).
  Préposé fédéral à la protection des données et à la transparence (PFPDT) – Protection des données
- **Formulaire de déclaration des cyberattaques (OFCS)**
  Signalement d'incidents en ligne pour les entreprises.
  Office fédéral de la cybersécurité (OFCS) – Formulaire de déclaration

Services de soutien spécifiques à l'industrie

- **CyberSeal – Label d'approbation de l'Alliance suisse pour la sécurité numérique**
  Récompense les prestataires de services informatiques qui garantissent un niveau de protection approprié – aide les PME à choisir des partenaires informatiques dignes de confiance.
  Alliance Sécurité Digitale Suisse - CyberSeal
- **GObugfree – Plateforme de piratage éthique et de détection de vulnérabilités**
  Solution permettant aux PME d'identifier et de signaler les vulnérabilités.
  GObugfree
- **ITsec4KMU – Prévention et défense contre les cyberattaques pour les PME suisses**
  Auto-évaluation et lignes directrices gratuites et axées sur la pratique pour les PME.
  ITSec4KMU
- **Suissedigital – Contrôle de sécurité PME**
  Contrôle de sécurité simplifiée pour les PME du secteur des communications numériques.
  Suissedigital – Contrôle de sécurité PME
- **ADN de cyberdéfense suisse (SCD-DNA)**
  Modèle pour l'enregistrement et l'amélioration systématiques de la cybersécurité des PME.
  SWISS CYBER DEFENCE DNA

Formation de sensibilisation et matériel de formation

- **Campagne SUPER**
  Campagne nationale pour la protection de base en cybersécurité – conseils faciles à comprendre pour les employés.
  Faites-le - La cybersécurité est S-U-P-E-R.ch
- **Cybernavi**
  Plateforme interactive d'information et de formation sur les cyberrisques, destinée spécifiquement aux PME et aux salariés.
  Cybernavi

Normes et standards (utiles pour l'évaluation des fournisseurs)

- **SNV – Association suisse de normalisation**
  Informations sur les normes ISO/IEC, notamment 27001, 27002 et 27701.
  Association suisse de normalisation - SNV

SQS – Organisme de certification pour la sécurité de l'information
Certifications, modèles d'audit et normes industrielles (par exemple, ISO 27001, normes de protection des données).
Association suisse pour la qualité et les systèmes de management | SQS SuisseCoordonnées en cas d'urgence

Police (cybercriminalité) :
Numéro d'urgence : 117. Les services de police cantonaux proposent des services spécialisés en matière de cybercriminalité.
www.fedpol.admin.ch

Office fédéral de la cybersécurité (OFCS) :
Formulaire de signalement des cyberincidents en Suisse : Signalement en ligne : Formulaire de déclaration OFCS

Conseils juridiques en cas de cyberincidents
De nombreux cantons et associations professionnelles proposent des services juridiques spécialisés. Autres possibilités:

- BDO Cybersécurité et Droit : www.bdo.ch
- Experts en protection des données : www.edoeb.admin.ch/fr

Glossaire

Authentification à deux facteurs (2FA)
Une couche de sécurité supplémentaire qui exige deux facteurs indépendants pour la connexion (par exemple, mot de passe + code SMS ou vérification via application).

Actif
Un actif précieux pour une entreprise dans le contexte informatique, par exemple les serveurs, les logiciels, les données ou les périphériques.

Sauvegarde
Une copie des données importantes, stockée séparément du système de production afin de pouvoir être restaurée après un incident.

Bluetooth
Technologie radio sans fil à courte portée. Les connexions Bluetooth ouvertes ou non sécurisées peuvent présenter un risque pour la sécurité.

Service cloud
Ressource informatique externe fournie via Internet (par exemple, Microsoft 365, Google Workspace). Nécessite des règles de sécurité et d'accès claires.

Cyberattaque
Tentatives de compromettre les systèmes informatiques, de voler ou de manipuler des données, ou de perturber les opérations.

CyberSeal

Label de qualité suisse distinguant les prestataires de services informatiques qui garantissent à leurs clients un niveau de protection adéquat contre les cyberrisques grâce à des mesures techniques et organisationnelles appropriées.

Violation de données
L'accès non autorisé, la perte ou la divulgation de données personnelles. Un signalement légal est requis en cas de risque pour les personnes concernées.

DLP (Prévention des pertes de données)
Outils ou politiques permettant d'empêcher la perte ou la divulgation illégale d'informations confidentielles.

Protection des terminaux
Logiciel de sécurité pour terminaux tels que les ordinateurs portables, les smartphones ou les serveurs. Détection des logiciels malveillants, des comportements suspects et des attaques.

Hacking éthique (piratage amical)
Scénario d'attaque autorisé dans lequel toutes les vulnérabilités concevables (techniques, organisationnelles, procédurales) sont examinées.
Les tests d'intrusion en font partie, mais de manière plus précise et plus claire.

Pare-feu
Un composant de sécurité qui surveille le trafic de données et bloque les accès non autorisés.

IoT (Internet des objets)
Les appareils connectés à Internet, tels que les caméras, les capteurs ou les routeurs, constituent souvent un point d'entrée pour les failles de sécurité en cas de non-mise à jour.

Gestion des appareils mobiles (MDM)
Logiciel pour la gestion centralisée et la sécurité des appareils mobiles tels que les smartphones ou les tablettes.

Logiciel malveillant
Logiciels malveillants tels que les virus, les chevaux de Troie ou les rançongiciels.

Segmentation du réseau
Diviser un réseau en zones distinctes pour limiter les attaques (par exemple, un réseau Wi-Fi invité séparer du réseau comptable).

Plan d'urgence (Plan d'intervention en cas d'incident)
Un document décrivant comment une entreprise doit réagir en cas de cyberincident.

Clés d'accès
Méthode d'authentification sans mot de passe utilisant des clés cryptographiques. Nettement plus sûre que les mots de passe traditionnels.

Gestion des correctifs
Mise à jour logicielle pour corriger les failles de sécurité. Gestion des correctifs = mise à jour systématique de tous les appareils et applications.

Test d'intrusion (Penetration Test)
Un test ciblé et précis qui identifie les faiblesses dans un domaine spécifique. Une approche structurée et méthodique.

Hameçonnage
Un message manipulateur (généralement un courriel) destiné à voler des identifiants, des données ou de l'argent.

Ransomware
Logiciel malveillant qui chiffre les données et exige une rançon.

Sauvegarde continue / sauvegarde hors ligne
Sauvegarde stockée séparément du réseau (par exemple, sur disque dur externe ou bande magnétique). Protection contre les ransomwares.

Ingénierie sociale
Manipulation de personnes pour obtenir des informations confidentielles ou un accès.

VPN (Réseau privé virtuel)
Connexion chiffréepermettant une communication sécurisée sur Internet.

WLAN (réseau local sans fil)
Réseau sans fil. Les réseaux Wi-Fi publics ou mal sécurisés peuvent faciliter les attaques.

Zéro confiance (Zero Trust)
Principe de sécurité : « Ne faites confiance à personne – vérifiez tout. » Aucune relation de confiance automatique n'est établie, ni à l'intérieur ni à l'extérieur de l'entreprise.