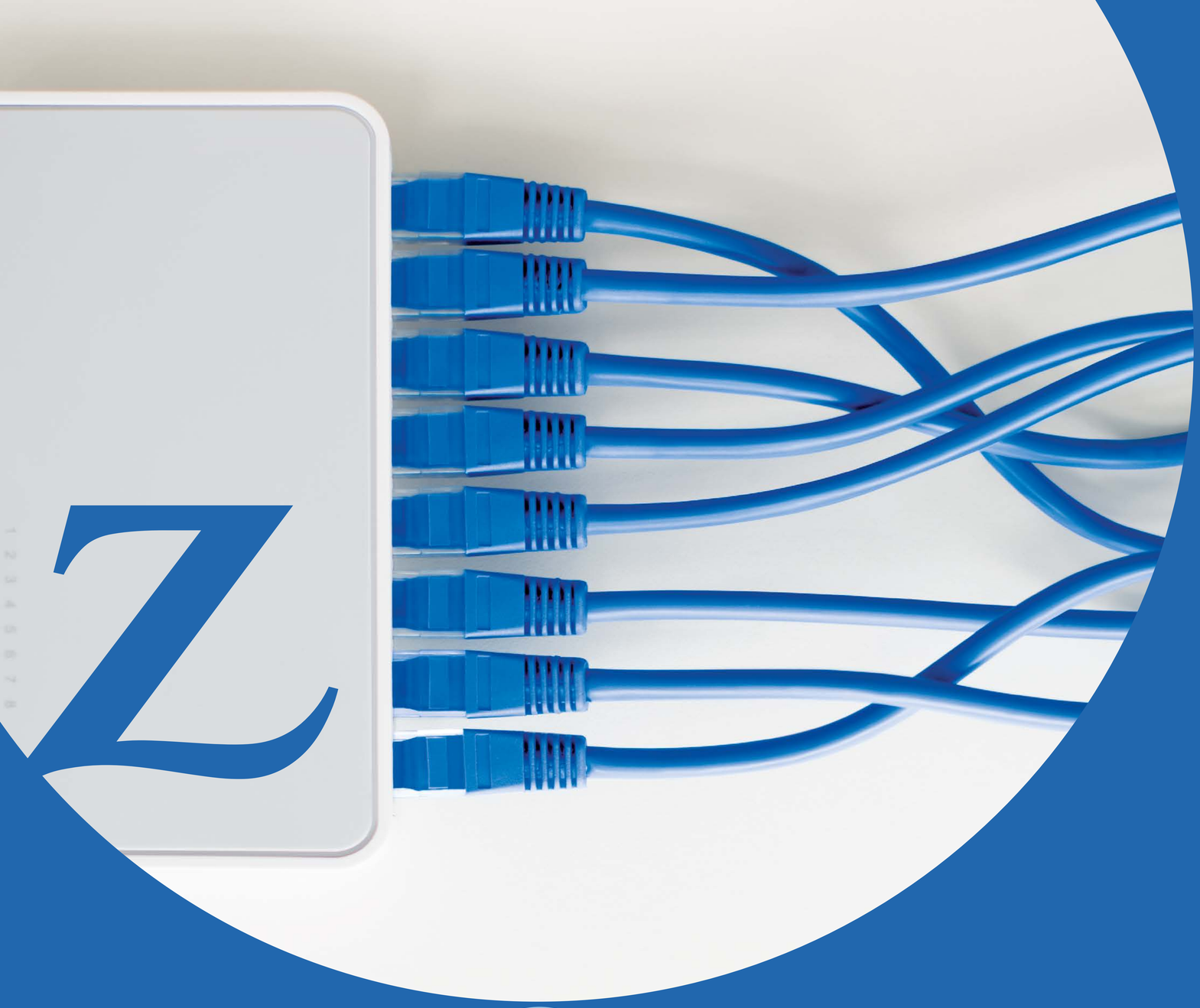


ZURICH

Brochure Cyber

Sommaire

La digitalisation – une opportunité qui ne vient pas sans risques
- Introduction
- Comparaison sectorielle

Astuces classiques des hackers
- Modèle d’attaque
- Portes d’entrée

Équipez-vous et réduisez vos risques
- Les 8 conseils essentiels
- Informations supplémentaires sur le thème

Le concept d’assurance de Zurich : Réduire les risques – couvrir le risque résiduel
- Étape 1 – Prévention
- Étape 2 – Protection contre les risques financiers
- Étape 3 – Gestion des sinistres

Exemples de sinistres

Contact

La digitalisation – une opportunité qui ne vient pas sans risques

La transition digitale offre de grandes opportunités aux PME suisses : Elles peuvent simplifier leurs processus existants, optimiser leurs produits et services et proposer une valeur ajoutée accrue à leurs clients. Cette transition requiert souvent la pleine attention de la direction de l'entreprise. Dans ce contexte, les cyberrisques sont souvent négligés et relégués au second plan. Pourtant, se protéger des cyberrisques est toujours crucial – afin que l'entreprise puisse exploiter pleinement le potentiel de la digitalisation et se prémunir des effets secondaires indésirables.

La membre du Conseil national Doris Fiala, qui préside les Swiss Cyber Security Days, en est convaincue : « La digitalisation est une immense opportunité, mais elle n'est pas exempte de risques. » Selon elle, d'après les extrapolations, la cybercriminalité occasionne des coûts à hauteur de 5 milliards de francs en Suisse chaque année. « C'est plus que le budget de l'Armée. » Doris Fiala l'a observé : beaucoup de PME suisses n'ont pas du tout conscience qu'elles pourraient également être touchées. « Face à la forte concurrence qui règne au quotidien, les PME doivent faire attention aux coûts et rechignent donc à dépenser de l'argent pour la cyber-sécurité. Pourtant, une bonne protection à tous les niveaux en vaut la peine. »

Une récente enquête de l'Institut gfs-zürich confirme elle aussi l'importance critique des cyberrisques pour les PME. Parmi les 500 chefs d'entreprise interrogés, un quart a indiqué avoir déjà été victime d'une cyberattaque ayant entraîné de lourdes conséquences.

La digitalisation – une opportunité qui ne vient pas sans risques

La digitalisation concerne tous les secteurs : dans toutes les entreprises ou presque, la majeure partie des communications et des tâches de bureau au quotidien ont lieu à l'aide de l'informatique. Suivant l'activité, les entreprises peuvent présenter différents talons d'Achille :

Professions libérales telles que les architectes ou ingénieurs

De nos jours, les ébauches, les planifications et les calculs sont entièrement informatisés, grâce à l'utilisation des programmes CAD par ex. Sans infrastructure informatique opérationnelle, toutes les activités sont suspendues.

Commerce et logistique

Les commandes, la gestion des stocks et la distribution sont représentés par des systèmes ERP. Les processus de vente aux clients finaux eux aussi se déroulent de plus en plus en ligne.

Hébergement, gastronomie et divertissement

Les commandes, la planification des horaires du personnel et l'ensemble de l'administration sont traités à l'aide de logiciels spécialisés. Les réservations et commandes ont lieu de plus en plus souvent en ligne, parfois également avec une application.

Services financiers

Toutes les transactions ou presque sont entièrement digitalisées – les versements, le négoce de titres et même les hypothèques sont exécutés ou renouvelés de plus en plus souvent en ligne.

Santé, accompagnement et travail social

Les traitements et la gestion des patients sont planifiés à l'aide de systèmes informatiques et reposent sur ceux-ci. Les dossiers de patients sont de plus en plus digitalisés, ce qui facilite le travail pour le personnel médical. Sans ces systèmes, plus grand chose ne fonctionnerait aujourd'hui.

Production

Suivant le secteur et l'entreprise, les processus de production reposent déjà en grande partie sur des installations automatisées et des robots. Si les commandes de ces installations ne fonctionnent plus, la production est à l'arrêt.

Astuces classiques des hackers

Modèle d’attaque

Les braquages de banques appartiennent au passé. Pour se procurer beaucoup d’argent, plus besoin de burin, de pistolet ou de voiture pour prendre la fuite. Il suffit d’une bonne connexion Internet, d’un esprit vif et de beaucoup d’énergie criminelle. «Modèles d’attaque» les plus fréquents des cybercriminels :

- Blocage des infrastructures informatiques
- Vol de données
- Attaque par déni de service (DoS)
- Cyberfraude

Portes d’entrée

Mais comment les cybercriminels parviennent-ils à accéder aux infrastructures informatiques pour lancer une attaque? Bien que les méthodes courantes des cybercriminels soient connues, elles leur permettent encore d’arriver à leurs fins. Parmi les portes d’entrée les plus courantes, on peut citer :

- accès à distance
- phishing
- infections drive-by
- systèmes non mis à jour ou mauvaises configurations
- tiers (par ex. prestataires externes)

Astuces classiques des hackers

Modèle d’attaque Portes d’entrée

Les braquages de banques appartiennent au passé. Pour se procurer beaucoup d’argent, plus besoin de burin, de pistolet ou de voiture pour prendre la fuite. Il suffit d’une bonne connexion Internet, d’un esprit vif et de beaucoup d’énergie criminelle. Mais alors, comment les hackers parviennent-ils à leurs fins concrètement ? Malgré la diversité et la finesse des cyberattaques, la majeure partie des cas de sinistres ayant lieu au quotidien suivent une poignée de modèles courants :

Blocage des infrastructures informatiques

Les cybercriminels s’introduisent dans les infrastructures informatiques pour les bloquer. Pour ce faire, ils utilisent souvent des programmes appelés « ransomwares » ou logiciels de rançon - et c’est ni plus ni moins ce dont il s’agit. Le hacker introduit un programme de cryptage des données et programmes au sein des infrastructures informatiques centrales (par ex. contrôleur de domaine Windows, système ERP). Ensuite, il contacte sa victime et l’informe qu’il ne lui communiquera la clé digitale pour déverrouiller et débloquer ses données et programmes qu’en l’échange d’une rançon. Souvent, le criminel ne se contente pas de bloquer les systèmes opérationnels, il verrouille également les systèmes de sauvegarde – par conséquent, de nombreuses entreprises concernées n’ont d’autre choix que de verser la rançon demandée.

Vol de données

Les cybercriminels s’introduisent dans les infrastructures informatiques, obtiennent des données sensibles et créent une copie de celles-ci. Les données clients sont particulièrement intéressantes pour les hackers – elles peuvent être utilisées pour différentes tentatives d’escroquerie. C’est notamment le cas pour les données de cartes de crédit ou les informations permettant d’usurper des identités (par ex. copies de pièces d’identité).

Astuces classiques des hackers

Modèle d’attaque Portes d’entrée

Attaque par déni de service (DoS)

Les cybercriminels submergent les canaux de communication électronique des entreprises avec des millions de demandes électroniques. Les systèmes concernés, sites Internet ou systèmes téléphoniques VoIP par exemple, sont surchargés et deviennent inutilisables. Généralement, pour ce type d’attaques, les hackers utilisent des réseaux de zombies – des milliers d’ordinateurs privés hackés au préalable – qui accèdent simultanément aux canaux de communication de la victime sur commande des hackers. Dans la plupart des cas s’ensuit là encore une demande de rançon. Si l’entreprise concernée ne souhaite plus être la cible de telles attaques à l’avenir, elle doit mettre la main à la poche.

Cyberfraude

Les hackers utilisent des canaux de communication électroniques pour inciter les collaborateurs à procéder à des virements d’argent et récupérer les sommes versées. Pour ce faire, ils inventent généralement des scénarios de crise – le criminel se présente par ex. en tant que CEO, CFO ou autre cadre dirigeant de l’entreprise. Souvent, ils utilisent des comptes e-mail compromis à cet effet. Il s’agit de comptes e-mails que le criminel s’est approprié en volant le nom d’utilisateur et le mot de passe. Cette technique est également appelée Business Email Compromise (BEC).

Astuces classiques des hackers

Modèle d’attaque **Portes d’entrée**

Quel que soit le type d’attaque, une réaction rapide est indispensable pour limiter les dégâts. Il convient également de réduire les risques d’incidents futurs à l’aide de mesures techniques ou organisationnelles. Bien que les méthodes courantes des cybercriminels soient connues, elles leur permettent encore d’arriver à leurs fins. Dans le prochain chapitre, nous décrirons les principales « portes d’entrée » des cybercriminels. Souvent, elles permettent même plusieurs modèles d'attaque:

Accès à distance

À l’ère du coronavirus, de nombreuses entreprises ont mis en place des outils pour que leurs collaborateurs puissent se connecter au système de l’entreprise en télétravail. Du véritable pain béni pour les cybercriminels du monde entier. En effet, seules les technologies d’accès à distance combinant une protection par mot de passe et une solution d’authentification multifactorielle offrent une sécurité élevée. C’est souvent le cas avec la technologie VPN. Mais de nombreuses entreprises sont refroidies par le coût du système et misent plutôt sur un système protégé uniquement par mot de passe. Le **Remote Desktop Protokoll (RDP)** est très fréquent dans ce contexte. Les cybercriminels reconnaissent ces interfaces RDP relativement rapidement et en essayant différentes combinaisons de noms d’utilisateurs et de mots de passe, ils parviennent à établir une connexion à distance. À partir de là, le hacker peut pénétrer plus loin dans le réseau afin de voler des données voire lancer une attaque de ransomware.

Phishing

Avec le phishing, le facteur humain est au centre puisque le collaborateur joue involontairement un rôle actif dans la cyberattaque. Le « phishing » est une forme particulière de social engineering, c.-à-d. de manipulation sociale. Le social engineering consiste à inciter les personnes à des actes qui leur nuiront. Si cette manipulation a lieu par e-mail, on parle généralement de phishing. Des e-mails de phishing incitent par exemple les collaborateurs à révéler des informations confidentielles ou à activer des logiciels malveillants sur leurs ordinateurs, en ouvrant une pièce jointe ou en cliquant sur un lien vers un site Internet par exemple. Ensuite, les criminels peuvent s’immiscer plus loin dans le réseau et voler des données ou lancer des attaques de ransomware.

Astuces classiques des hackers

Modèle d'attaque **Portes d'entrée**

Infections drive-by
Dans de nombreuses entreprises, les applications sont mises à jour trop peu souvent. Généralement, on utilise des navigateurs présentant des points faibles bien connus, au niveau des « plugins » par exemple. Dans ce cas, il suffit qu'un collaborateur visite un site Internet piraté ou « malveillant ». Celui-ci identifie le point faible dans le navigateur et s'introduit dans le système informatique de la victime. La visite d'un site Internet falsifié peut donc suffire pour transférer des logiciels malveillants à une entreprise.

Systèmes non mis à jour ou mauvaises configurations :
Aujourd'hui, toutes les entreprises ou presque exploitent une multitude de systèmes informatiques directement reliés à Internet, et qui sont donc accessibles depuis n'importe où dans le monde. Ces systèmes se composent d'un système d'exploitation ainsi que d'applications souvent nombreuses. Par conséquent, la plupart des entreprises sont débordées par la nécessité de maintenir leurs systèmes à jour en permanence – d'autant plus que de nouvelles mises à jour et « patches de sécurité » sont publiés par les fabricants de logiciels tous les jours ou presque. Par conséquent, il arrive que les lacunes de sécurité ne soient pas comblées avant des mois voire des années. Dès qu'un cybercriminel identifie de telles failles de sécurité, il peut les exploiter (via la technique appelée « Exploit ») et obtenir un accès aux données ou même prendre le contrôle des systèmes.

Tiers (par ex. prestataires externes)
Lorsque les « portes d'entrée » sont ciblées via un accès à distance, le phishing, les infections drive-by ou les systèmes non mis à jour, l'entreprise est victime d'une attaque directe. Mais les cybercriminels peuvent également exploiter les points faibles de tiers. Si une entreprise partage des données sensibles avec un prestataire ou qu'elle achète des prestations logicielles à des prestataires, elle est exposée à ses propres risques de sécurité, mais aussi à ceux du prestataire.

Équipez-vous et réduisez vos risques

Les 8 conseils essentiels Informations supplémentaires sur le thème

Même si chaque entreprise est unique, nous avons résumé les principaux conseils pour vous :

1. L'analyse de risque en tant que tâche de management : Quels sont mes « joyaux les plus précieux » et comment les protéger ? Cela comprend également une gestion de crise professionnelle avec plan d'urgence pour les cyberattaques.

2. Formez vos collaborateurs au traitement des données et des e-mails car ce sont les premières portes d'accès pour les logiciels malveillants et les attaques.

3. Vérifiez les droits d'accès une fois par an et à chaque changement de poste des collaborateurs : cela évitera par exemple que d'anciens collaborateurs accèdent au réseau.

4. Adoptez des mots de passe intelligents qui combinent des caractères spéciaux, des chiffres et des lettres, comportent au moins huit signes et n'incluent pas votre nom ou votre date de naissance. Évitez d'utiliser plusieurs fois le même mot de passe, renouvelez les mots de passe régulièrement et ne les communiquez pas à des tiers.

5. Assurez-vous que les accès à distance soient bien protégés eux-aussi et qu'ils soient couplés à une solution d'authentification multifactorielle. Il est également conseillé de limiter les accès externes dans la durée et dans l'espace, par ex. de les limiter à certaines adresse IP, à des horaires bien précis (par ex. opérations de maintenance).

6. Veillez à ce que votre système d'exploitation soit toujours à jour car les hackers s'attaquent aux points faibles des logiciels. Cela implique notamment de changer de système d'exploitation lorsqu'il est trop vieux, comme par exemple Windows XP et Windows 7, qui ne sont plus mis à jour. Il est également indiqué de réaliser un inventaire de tous les ordinateurs et applications utilisés par l'entreprise afin d'obtenir un aperçu de tous les systèmes informatiques en service.

7. Installez des antivirus qui détectent et bloquent les logiciels malveillants et dressent un pare-feu contre les accès illicites. Les programmes doivent être mis à jour quotidiennement.

8. Effectuez des sauvegardes de données régulières, tous les jours ou même plus souvent s'il s'agit de données sensibles. La nouvelle sauvegarde ne doit pas écraser la précédente puisque dans ce cas, les données historiques peuvent être perdues. Logique, mais essentiel : Une copie de la sauvegarde doit être extraite du réseau en permanence, afin qu'un cybercriminel ne puisse pas y accéder en cas d'attaque. Testez régulièrement le fonctionnement de la sauvegarde des données.

Équipez-vous et réduisez vos risques

Vous souhaitez obtenir davantage d'informations quant aux méthodes de réduction des cyberrisques pour votre entreprise ? Alors nous vous recommandons les sources d'informations détaillées suivantes :

Avec la plateforme digitale « **Zurich Risk Advisor** », vous pouvez procéder à une auto-évaluation de vos cyberrisques. L'évaluation comprend cinq modules et vous soumet des propositions d'amélioration concrètes. Informez-vous sur notre site Internet (en anglais) et téléchargez l'application : **Lien**

Le **centre national pour la cybersécurité (NCSC)** est le centre de compétences de la Confédération en matière de cybersécurité. Cette autorité a pour but de protéger les citoyens suisses des cyberrisques. Sur sa page d'information à destination des entreprises, le NCSC avertit des risques actuels et propose une vue d'ensemble complète des méthodes avec lesquelles les entreprises peuvent se protéger des cyberrisques. **Lien**

L'association faîtière de l'économie digitale en Suisse **ICT Switzerland** souhaite elle aussi aider les PME suisses à réduire les cyberrisques; elle a rédigé un guide à ce propos: **Lien**

Le concept d’assurance de Zurich

1 Prévention

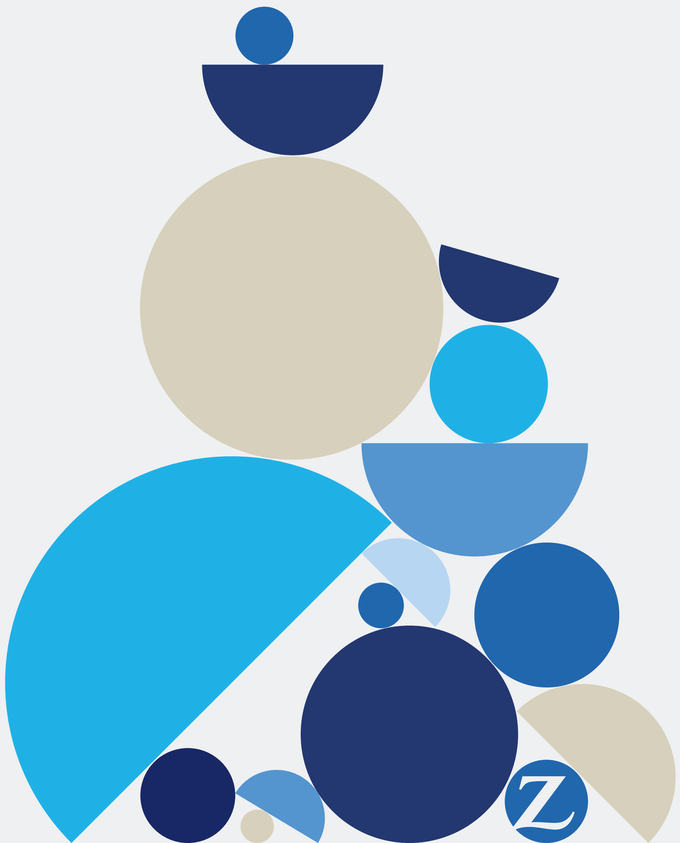
Le concept de cyberassurance Zurich vous aide à comprendre les risques et à vous protéger des cyberattaques.

2 Protection contre les risques financiers

Nos modules de couverture vous permettent de composer la solution d’assurance qui vous correspond.

3 Gestion des sinistres

Une intervention rapide et adaptée en cas de pépin est déterminante pour la réussite des mesures.



Le concept d’assurance de Zurich

Le concept de cyberassurance Zurich vous aide à comprendre les risques et à vous protéger des cyberattaques. En coopération avec notre partenaire, nous vous aidons à réduire les cyberrisques pour votre entreprise.

Formation sur la cybersécurité : afin que vos collaborateurs ne deviennent pas complices

En matière de cybersécurité, l’erreur est bien souvent humaine. Quel que soit le type d’entreprise, les e-mails de hackers non repérés sont la porte d’entrée la plus fréquemment utilisée pour les cyberattaques ciblées. Et c’est précisément là que Zurich peut intervenir avec sa Formation sur la cybersécurité gratuite pour les clients Cyber de Zurich et leurs collaborateurs. La formation en ligne a été développée par notre partenaire SoSafe – elle met l’accent sur l’e-learning et la cybersécurité. Les cinq modules de modules de Base ainsi que la simulation de phishing sensibilisent les collaborateurs aux risques d’Internet et évitent ainsi qu’ils deviennent involontairement complices.

Évaluation des risques

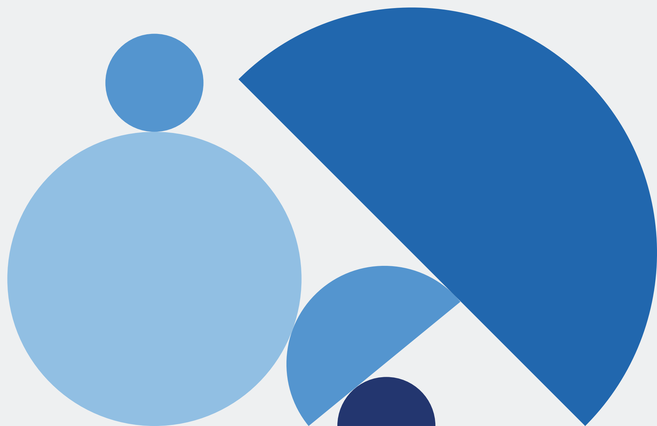
Ensemble avec Spie ICS, un des leaders des technologies de l’information et de la communication en Suisse, Zurich a développé un Security Check et une évaluation de sécurité. Ces deux analyses ont pour but d’identifier vos risques de cybersécurité, de les évaluer et de proposer des recommandations de mesures. Elles sont réalisées par les experts de Spie.

Security Check (1 heure de travail pour vous)
L’analyse a lieu sur place dans vos locaux. Avec l’assistance d’un outil, vos systèmes et applications sont analysés afin de détecter les points faibles. Vous recevez un rapport détaillant la gravité des points faibles ainsi que les mesures de correction/réduction.

Évaluation de sécurité (2 heures de travail pour vous)
L’analyse complète des processus de sécurité et les contrôles de la confidentialité, de l’intégrité et de la disponibilité des systèmes/applications sont effectués sur place, dans vos locaux. Un entretien structuré a lieu avec vous.

Vous recevez un rapport détaillé contenant les informations suivantes :
– Statut des contrôles de sécurité
– Points faibles identifiés
– Recommandations pour la réduction des risques.

En tant que client Cyber de Zurich, vous profitez de conditions spéciales pour la réalisation d’un Security Check ou d’une évaluation de sécurité chez Spie ICS. Les coûts sont fonction du nombre de postes de travail informatiques : le Security Check est proposé dès CHF 630.- (jusqu’à 10 postes de travail) et l’évaluation de sécurité à partir de CHF 1'600.- (jusqu’à 10 postes de travail).



Le concept d’assurance de Zurich

Nos modules de couverture vous permettent de composer la solution d’assurance qui vous correspond.

Malheureusement, même un concept solide en matière de cybersécurité n’est pas la garantie d’une protection absolue contre les cyberattaques. Si vous êtes tout de même victime d’une cyberattaque, Zurich vous offre une couverture d’assurance optimale et vous aide à maîtriser les conséquences.

Choisissez la formule idéale pour votre entreprise :

Basic dès CHF 410	Cyber-restauration des données et des systèmes Cyber-gestion de crise Cyber-responsabilité civile Cyber-protection juridique
Optimum dès CHF 690	+ Cyber-perte d’exploitation
Premium dès CHF 845	+ Cyber-Crime

Le concept d'assurance de Zurich

Cyber-restauration des données et des systèmes

- Clarifications techniques ou analyses informatiques légales : Que s'est-il passé précisément ?
- Restauration ou récupération de données et informations
- Récupération de matériel endommagé (bricking)
- Identification des points faibles du logiciel et mesures d'amélioration de la sécurité (betterment)
- Paiements extorqués par chantage et coûts pour la défense contre le cyber-chantage
- Prise en charge des coûts en cas de hacking téléphonique

Basic Optimum Premium

Cyber-gestion de crise

- Vérification des obligations de déclaration et d'information
- Information des personnes concernées sur une base volontaire
- Procédures administratives et amendes et pénalités (assurables)
- Pénalités contractuelles en cas de manquement aux PCI DSS-Standards
- Call center, gestion des cartes de crédit et des identités pour les personnes concernées
- Actions « Goodwill » telles que des rabais et remises sur les prix pour les personnes concernées
- Planification et mise en œuvre de campagnes de relations publiques en cas d'échos négatifs dans les médias

Basic Optimum Premium

Cyber-responsabilité civile

Indemnisation et contestation des prétentions injustifiées en cas de/en lien avec :

- La perte, le vol ou la publication de données – indépendamment du type de cyberattaque
- Une violation de la loi sur la protection des données (y compris RGPD)
- Atteinte au nom, aux droits d'auteur et aux droits des marques
- Frais de procédure et honoraires d'avocat

Basic Optimum Premium

Cyber-protection juridique

- Conseil concernant les mesures juridiques d'urgence
- Actions en dommages et intérêts
- Défense pénale en cas de violation par négligence des dispositions de protection des données

Basic Optimum Premium

Cyber-perte d'exploitation et frais supplémentaires

- En raison d'une cyberattaque ou d'une erreur d'utilisation
- En raison d'une ordonnance des autorités suite à une violation de la protection des données
- Couverture de la perte de gain nette et des frais supplémentaires liés au maintien de l'exploitation

Optimum Premium

Cyber-Crime

- Cyber-escroquerie consécutive à des actes frauduleux commis par des tiers (Social engineering)
- Cyber-vol par manipulation des systèmes informatiques par des tiers (E-banking hacking)

Premium

Le concept d’assurance de Zurich

Une intervention rapide et adaptée en cas de pépin est déterminante pour la réussite des mesures.

En cas de sinistre, il faut réagir sans attendre. C’est pourquoi notre hotline est disponible 7 jours/7, à toute heure. Durant les horaires de bureau, nos collaborateurs spécialisés en cyberattaques s’occuperont de votre cas. En dehors de ces horaires, votre appel sera directement transféré à notre partenaire informatique Compass Security.

Suivant les besoins, nous organiserons l’intervention d’experts pour vous. Dans ce contexte, nous collaborons également avec l’entreprise de sécurité informatique Compass Security. Grâce à son expérience et son savoir-faire, notre partenaire est parfaitement armé pour trouver une solution rapide et durable à votre cyberattaque. D’après l’analyse des causes, elle vous recommandera également des mesures afin de garantir une cyberprotection durable. Ainsi, vous pourrez apporter une protection complète à votre entreprise à l’avenir.

Nous vous aidons non seulement dans le cadre de vos problèmes informatiques, mais aussi via les bons partenaires lorsqu’il est question de thèmes juridiques, pour contrôler une obligation d’information par ex., ou prendre en charge la défense contre des prétentions en dommages et intérêts ou le dépôt de recours pénaux. La réputation de l’entreprise peut rapidement être en jeu elle aussi. C’est pourquoi en cas de souci, nous recourons à des spécialistes pour la communication à l’égard des parties externes et vous aidons à protéger votre image.

Le concept d’assurance de Zurich

Processus de sinistres Cyber : Le cas de sinistre est le « moment de vérité » – conformément à notre promesse « à vos côtés lorsque vous en avez besoin. »

Conclusion du contrat

Toutes nos félicitations pour la souscription de votre cyberassurance Zurich. Nous nous tenons à votre entière disposition en cas de questions et vous proposons une formation de sensibilisation gratuite à destination de vos collaborateurs, ainsi qu’une évaluation des risques cyber en tant que service facultatif.

Événements

Vous identifiez des anomalies dans votre système IT ou vous avez été victime d’une cyberattaque.

Déclaration

Déclarez-nous l’événement en toute simplicité, 24h/24 et 7 j/7 au :

044 629 10 40

zurich.ch/déclarer-un-sinistre

Nous nous ferons un plaisir de clarifier les faits avec vous et de discuter de la marche à suivre.

Mesure

Si besoin, Zurich vous met en relation avec un spécialiste informatique, qui initiera les mesures immédiates et/ou assurera la correction des défauts dans son intégralité. À défaut de quoi, vous pouvez commissionner votre propre partenaire IT pour la résolution du problème.

Traitement

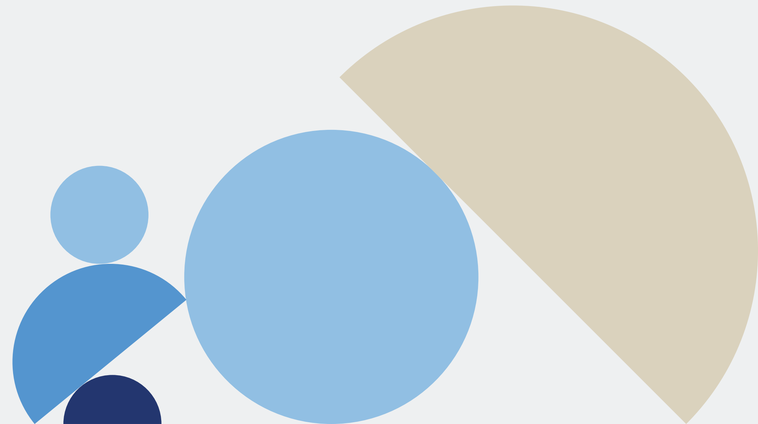
Zurich examine le rapport d’analyse du spécialiste IT. Elle détermine l’indemnisation.

Règlement

Nous discutons du règlement du sinistre ensemble. Avec l’avis de règlement, vous recevez un relevé des coûts et une confirmation de paiement du sinistre.

Dommages consécutifs

En tant que service en option, nos spécialistes IT peuvent vous fournir des conseils de prévention.



Exemples de sinistres : cabinet médical (1/2)

Vol de données dans un cabinet médical suite à l'attaque de son prestataire informatique par un hacker

1 La situation initiale

Le c**abinet médical** Médecins Dupont Sàrl est un cabinet de groupe exploité par plusieurs pédiatres

Chiffre d'affaires annuel CHF 1'500'000
Nombre de collaborateurs 6

L'infrastructure informatique (y compris le système de gestion des patients) est mise à disposition par un prestataire informatique. Les collaborateurs utilisent des ordinateurs portables reliés au serveur. Les données sont enregistrées directement sur le serveur.

2 Scénario de sinistre

Suite à une cyberattaque ciblée contre le prestataire informatique du cabinet médical Médecins Dupont Sàrl, des personnes non autorisées accèdent aux données des patients. Les médecins ne savent pas de quelles données il s'agit et les méfaits que le hacker pourrait commettre avec celles-ci.

3 En quoi la

formule Basic de Zurich peut aider

Gestion des sinistres

- Zurich s'informe auprès du preneur d'assurance afin de déterminer si son prestataire informatique a besoin d'aide pour corriger le dommage. Ce dernier est déjà en train de clarifier les faits et de rétablir le fonctionnement de l'infrastructure informatique. Toutefois, il apparaît bientôt que l'intervention d'un expert sera nécessaire pour évaluer l'étendue du sinistre. Zurich organise rapidement l'assistance nécessaire afin de clarifier les données de patients concernées par la cyberattaque.
- Par le biais de ses partenaires, Zurich offre également aux médecins un conseil juridique compétent concernant l'obligation d'information et la responsabilité. Avec la révision prévue de la loi sur la protection des données et les risques juridiques accrus qui découlent des réglementations plus strictes, l'expertise spécialisée est d'autant plus importante.
- Dans le cadre de la gestion des sinistres, les experts du partenaire de relations public de Zurich aident le cabinet médical à informer toutes les personnes de façon adaptée.

Exemples de sinistres : cabinet médical (2/2)

Protection contre les risques financiers

- Module Cyber-restauration des données et des systèmes
  Le partenaire d'analyse informatique de Zurich analyse la situation afin de déterminer l'ampleur du sinistre et vérifie les données de patients concernées. Suite à l'analyse, l'expert informatique peut évaluer les dommages que le hacker pourrait causer avec les données. Si les données n'étaient pas suffisamment protégées, on peut supposer que le hacker les mettra en vente sur le darknet. Si les données et systèmes du cabinet médical ont été corrompus, Zurich prend en charge les coûts de la restauration des données et de l'infrastructure informatique.

- Module Cyber-protection juridique
  Il convient de déterminer dans quelle mesure les patients ou les autorités concernés doivent être informés du vol des données. L'analyse initiale est couverte par la protection juridique.

- Module Cyber-responsabilité civile
  Si l'analyse juridique initiale révèle qu'aucun droit n'a été enfreint, Zurich vous aide à vous défendre contre les prétentions en responsabilité civile injustifiées. Si les données personnelles n'étaient pas suffisamment protégées, il existe un risque que les prétentions en responsabilité civile soient justifiées et exécutées. Dans ce cas, Zurich verse les dommages et intérêts correspondants.

- Module Cyber-gestion de crise
  Une stratégie de communication adaptée est développée d'après les conclusions de l'analyse du dommage. Les coûts de communication sont supportés par Zurich. Si l'analyse juridique initiale révèle qu'aucune infraction n'a été commise, les coûts liés à la communication vis-à-vis des autorités sont également assurés.

- Aperçu des coûts assurés dans cet exemple
  Coûts de l'analyse informatique, des conseillers en communication et éventuels coûts supplémentaires pour le conseil juridique/le règlement des litiges, en fonction de la situation (la déduction de la franchise demeure réservée, selon convention)

Exemples de sinistres : fabricants (1/2)

Arrêt de la production chez un fabricant de pièces métalliques suite à un accès à distance

1 La situation initiale

Le **fabricant** Durant Pièces Métalliques SA propose une offre universelle de pièces métalliques et des délais de livraison rapides.

Chiffre d'affaires annuel CHF 3'000'000
Nombre de collaborateurs 15

L'intégralité de **l'infrastructure informatique** se situe dans les locaux de l'entreprise ; outre le réseau administratif de l'entreprise, celle-ci possède également un réseau dédié aux équipements de production. Les machines sont accessibles à distance via Internet, afin que le fabricant puisse assurer leur maintenance en permanence.

2 Scénario de sinistre

Un dimanche, un hacker s'introduit dans le réseau interne de l'entreprise par accès à distance, après avoir volé un mot de passe. Il bloque l'ensemble de l'infrastructure informatique et met toutes les machines de production à l'arrêt. Pendant 5 jours, l'entreprise n'a plus la possibilité de produire ses pièces métalliques. Tandis que le prestataire informatique local tâche de nettoyer le réseau des virus et de redémarrer les machines de production en collaboration avec le fabricant de celles-ci, l'entrepreneur reçoit un appel d'un client important. Celui-ci souhaite passer une commande urgente d'un volume de CHF 80'000, dans un délai de 7 jours. Comme le délai ne peut pas être prolongé, l'entrepreneur est contraint de refuser la commande à cause de la cyberattaque. De plus, il doit déjà terminer une commande en cours sous 10 jours. Pour y parvenir, tous les collaborateurs de la production vont devoir faire des heures supplémentaires le weekend.

Dans la mesure où le prestataire informatique de l'entreprise ne possède pas lui-même les compétences nécessaires à l'analyse et à la correction du dommage, l'entreprise a besoin d'une aide extérieure. L'entrepreneur vient immédiatement demander son aide à Zurich.

3 En quoi la **formule Optimum** de Zurich peut aider

Gestion des sinistres
La ligne d'assistance dommages pour les cyberattaques est joignable 24h/24 et 7j/7, si bien que le fabricant peut déclarer le sinistre à Zurich dès le dimanche soir. Pendant les horaires de bureau, nos collaborateurs spécialisés en cyber-dommages s'occupent de l'attaque. En dehors de ces horaires, l'appel est directement transféré à notre partenaire informatique, qui cherche alors une solution au problème. Après l'appel, notre partenaire s'assure qu'une équipe Incident-response soit sur place chez le client pour tâcher de trouver une solution

Exemples de sinistres : fabricants (2/2)

Protection contre les risques financiers

- Module Cyber-restauration des données et des systèmes
  La cyberattaque provoque des coûts à hauteur de CHF 4’000 pour le prestataire informatique local. CHF 7’000 supplémentaires sont dus au titre des travaux de maintenance du fabricant des machines suite à la cyberattaque. Les coûts pour l’intervention rapide de l’équipe incident-response afin de restaurer l’infrastructure informatique et d’éliminer le point faible s’élèvent à CHF 13’000.

- Module Cyber-perte d’exploitation
  Le logiciel malveillant introduit sur le réseau de l’entreprise bloque l’accès aux machines de production pendant cinq jours. En raison de la commande qui n’a pas pu être acceptée, la perte de chiffre d’affaires s’élève à CHF 60’000 (CHF 80’000 pour la commande moins CHF 20’000 correspondant aux coûts économisés (matières premières, électricité, etc.)). La charge de travail supplémentaire pour la deuxième commande qui ne pourra être honorée qu’avec des heures supplémentaires le weekend est également couverte. Un montant supplémentaire de CHF 5'000 doit être versé au personnel de production au titre de ces horaires exceptionnels.

- Aperçu des coûts assurés dans cet exemple
  CHF 89’000 (la déduction de la franchise demeure réservée, selon convention)

Exemples de sinistres : fiduciaires (1/2)

Vol de comptes clients d'une société fiduciaire suite à une attaque de phishing

1 La situation initiale

La **société fiduciaire** Martin Fiducie SA exécute des paiements pour le compte de ses clients.

Chiffre d'affaires annuel CHF 6'500'000
Nombre de collaborateurs 22

L'infrastructure informatique est mise à disposition par un prestataire informatique. Les collaborateurs utilisent des ordinateurs portables reliés au serveur. Les données sont enregistrées directement sur le serveur.

2 Scénario de sinistre

Un collaborateur est victime d'une attaque de phishing. Il reçoit une supposée candidature spontanée et clique sur la pièce jointe, sensée être le dossier de candidature. Il charge alors involontairement un logiciel malveillant sur son appareil. Avec ce logiciel, le hacker peut prendre le contrôle lorsque le collaborateur se connecte au portail e-banking et détourner des fonds des comptes bancaires des clients.

3 En quoi la **formule Premium** de Zurich peut aider

Gestion des sinistres
Après que le fiduciaire a déclaré le dommage à Zurich, les cyber-spécialistes de Zurich prennent immédiatement contact avec le prestataire informatique de l'entreprise. En outre, ils assistent la fiduciaire dans la communication avec les autorités. Le prestataire informatique reprend rapidement la maîtrise de la situation et en l'espace de trois jours ouvrables, il parvient à éliminer les logiciels malveillants des systèmes. Afin de garantir que le hacker ne puisse plus accéder aux systèmes, Zurich propose également l'analyse informatique par une entreprise partenaire de Zurich. Celle-ci examine l'ensemble des systèmes pour retrouver les traces de l'attaque. L'analyse révèle que le hacker ne peut plus accéder au système et qu'aucune donnée client n'a été volée.

Exemples de sinistres : fiduciaires (2/2)

Protection contre les risques financiers

- Module Cyber-restauration des données et des systèmes
  Les coûts pour le nettoyage des systèmes et l’élimination des points faibles s’élèvent à CHF 12’000 (coûts pour le prestataire informatique et l’analyse informatique).

- Module Cyber-gestion de crise
  Zurich et ses partenaires aident les clients dans la communication vis-à-vis des autorités.

- Module Cyber-Crime
  Un montant total de CHF 130'000 a été volé aux clients du bureau de fiducie depuis un compte administré par l’assuré. Le fiduciaire est on ne peut plus soulagé lorsqu’il constate que le sinistre ne dépasse pas sa somme d’assurance

- Aperçu des coûts assurés dans cet exemple
  CHF 142’000 (la déduction de la franchise demeure réservée, selon convention)

Zurich Cyberassurance

Contact et avantages

La digitalisation offre de nombreuses opportunités de croissance aux entreprises. Avec Zurich, vous êtes parfaitement protégé pour exploiter pleinement ce potentiel – grâce aux mesures préventives, à une couverture complète des risques financiers ainsi qu’à une gestion de sinistres compétente.

Pour plus d’informations sur la Zurich Cyberassurance, rendez-vous sur notre **site Internet**. Nous nous ferons un plaisir de vous conseiller personnellement.

Adressez-vous à l’agence Zurich la plus proche ou appelez-nous gratuitement au **0800 80 80 80** ou prenez directement contact avec votre courtier/agence.

Avantages de la Zurich Cyberassurance

- Nous vous aiderons volontiers à protéger votre entreprise contre les cyberrisques - avec une formation à la cybersécurité gratuite pour vos collaborateurs ainsi qu’une évaluation des risques détaillée par notre entreprise partenaire Spie, qui propose des conditions préférentielles aux clients Zurich.
- Les couvertures sont décrites de façon claire et simple. Ainsi, vous savez à tout moment ce qui est assuré ou non.
- Les couvertures supplémentaires complètes tiennent compte des besoins et nouveaux risques spécifiques à chaque secteur.
- Grâce à nos spécialistes Zurich ainsi qu’à notre réseau professionnel de partenaires, Zurich peut vous prêter main forte avec compétence en cas de problème, mais vous restez libre de faire appel aux prestataires de votre choix.
- Nous nous occupons non seulement de la correction du problème, mais recherchons également les causes et vous aidons à éliminer le point faible pour le futur également.
- L’offre a été conçue pour les petites et moyennes entreprises.