Cybercriminalité

La sécurité informatique fait partie de la sécurité de l'entreprise.

Ces derniers mois divers cas de cyberattaques ont été signalés et traités dans les médias. Le sujet reste néanmoins toujours d'actualité et concerne également les entreprises de notre branche.

Stadler Rail a fait savoir que son réseau IT a été attaqué par un logiciel malveillant début mai. L'auteur inconnu a tenté de faire chanter le constructeur thurgovien de véhicules ferroviaires en exigeant une importante rançon. En menaçant l'entreprise de publier les données volées, il voulait la mettre sous pression et lui nuire. La poursuite de la production et des services a toutefois pu être garantie. Le groupe a immédiatement déployé les mesures de sécurité nécessaires, mobilisé des spécialistes externes et impliqué les autorités compétentes. Les données de sauvegarde étaient disponibles intégralement et fonctionnelles.

Ce type d'incident n'est pas rare et ne touche pas que les grandes entreprises; les PME sont de plus en plus exposées aux cyberattaques et constituent des cibles intéressantes pour les criminels, même s'ils cherchent moins à y voler des données ou des informations. Ils cherchent plutôt à bloquer entièrement l'entreprise, p. ex. en cryptant l'ensemble de l'infrastructure IT. Le cybercriminel qui y parvient exige alors une rançon, parfois colossale, pour que les données puissent à nouveau être décryptées. Les conséquences peuvent s'avérer fatales et conduire une entreprise à la faillite. Souvent, les petites entreprises ne disposent d'aucun service de sécurité informatique et organisent elles-mêmes leur infrastructure IT. Généralement rudimentaire, celle-ci est alors une cible facile.

Un clic suffit

La Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI du Centre national pour la cybersécurité (NCSC) observe une augmentation des attaques de phishing sous forme d'e-mails frauduleux demandant au destinataire d'introduire ses identifiants dans le but d'accéder à des données sensibles. Les e-mails peuvent aussi contenir des documents contenant un logiciel malveillant. Ces derniers mois p. ex., des e-mails annonçant un remboursement d'impôt ont été envoyés. Pour en bénéficier, il fallait ouvrir un fichier Excel. Il ne faut jamais ouvrir un tel document, mais supprimer l'e-mail immédiatement sans y répondre. Les e-mails frauduleux sont le plus souvent repérables. Ils contiennent p. ex. une adresse e-mail obscure, des fautes d'orthographe, des adresses impersonnelles, des pièces jointes douteuses ou ils invitent à cliquer sur un lien. Une banque ne demanderait par exemple jamais d'informations clients par e-mail. Ne pas ouvrir les e-mails suspects n'est qu'une mesure de sécurité parmi d'autres. Ainsi, voici d'autres gestes à adopter.

- **Ne transmettre des données sensibles que par un site crypté:** Ces sites sont reconnaissables par leur URL commençant par https:// (s = security).
- **Protéger le site Internet:** Les entreprises qui disposent d'un site Internet s'exposent à des dangers particuliers. Un CMS (Content Management System) est une cible de choix. S'assurer d'avoir toujours la version la plus récente installée permet de réduire les risques.
- **Sauvegarder les données régulièrement.**
- **Définir une politique de mots de passe:** Les mots de passe doivent être changés régulièrement. Les mots de passe forts contiennent au minimum 12 caractères et comprennent des majuscules, des minuscules, des chiffres et des

AM Suisse führt zum Thema «Cyberkriminalität» im November Abendveranstaltungen durch:

go4office: «Internet Kriminalität – Nein Danke!»
Informieren Sie sich, wie Sie sich sinnvoll vor Cyberangriffen schützen und welche Möglichkeiten und Versicherungen es gibt, die Sie unterstützen, wenn Ihr Unternehmen trotz aller Vorsicht angegriffen wird.

Termine
- 24. November 2020, 17.00 bis 19.30 Uhr, Geschäftsstelle AM Suisse, Zürich
- 26. November 2020, 17.00 bis 19.30 Uhr, AM Suisse Bildungszentrum Aarberg

Kosten
CHF 60.– für AM Suisse-Mitglieder (Unkostenbeitrag)
CHF 120.– für Teilnehmer anderer Firmen

Kurssprache: Deutsch
Anmeldeschluss: 4 Wochen vor Kursbeginn

Weitere Informationen
amsuisse.ch/bildung/kursprogramm oder
E-Mail: s.kernen(at)amsuisse.ch
Tel: +41 044 285 77 04

En novembre, l'association patronale AM Suisse organise des soirées en allemand consacrée à la « cybercriminalité » :

go4office : « Internet Kriminalität – Nein Danke! »
Informez-vous sur les moyens disponibles pour vous protéger convenablement contre les cyberattaques et sur les possibilités et assurances existantes si votre entreprise y est confrontée malgré toutes vos précautions.

Dates
- 24 novembre 2020, de 17 h 00 à 19 h 30, secrétariat d'AM Suisse, Zurich
- 26 novembre 2020, de 17 h 00 à 19 h 30, Centre de formation d'AM Suisse à Aarberg

Coûts
- CHF 60.– pour les membres d'AM Suisse (participation aux frais)
- CHF 120.– pour les participants d'autres entreprises

Langue du cours: allemand
Date limite d'inscription: 4 semaines avant le début du cours

Informations complémentaires :
www.amsuisse.ch/fr/formation/programme-des-cours ou
e-mail : s.kernen@amsuisse.ch
tél. : +41 044 285 77 04.

Cyberkriminalität

IT-Sicherheit gehört zur Unternehmenssicherheit

In den letzten Monaten wurden verschiedene Fälle von Cyberkriminalität bekannt und in den Medien behandelt. Das Thema ist aber dauernd aktuell und betrifft auch alle Unternehmen unserer Branche.

Das IT-Netzwerk von Stadler Rail wurde Anfang Mai 2020 mit Schad-Software angegriffen, wie das Unternehmen mitteilte. Die unbekannte Täterschaft versuchte, den Thurgauer Schienenfahrzeug-Hersteller unter Forderung hoher Geldbeträge zu erpressen. Mit der möglichen Veröffentlichung von gestohlenen Daten wollte sie das Unternehmen unter Druck setzen und ihm schaden. Trotzdem war die Weiterführung der Produktion und der Dienstleistungen weiterhin gewährleistet. Der Konzern leitete sofort die erforderlichen Sicherheitsmassnahmen ein, zog externe Spezialisten bei und involvierte die zuständigen Behörden. Die Backup-Daten waren weiterhin vollumfänglich vorhanden und funktionsfähig.

Existenzbedrohende Forderungen

Vorfälle wie diese sind nicht selten. Sie betreffen nicht allein Grossunternehmen. Auch KMU sind zunehmend Cyberangriffen ausgesetzt und für Kriminelle attraktive Ziele. Es geht dabei weniger um Daten oder Informationen, die gestohlen werden. Vielmehr erwirken die Angreifer den kompletten Ausfall einer Unternehmung, beispielsweise durch die Verschlüsselung der gesamten IT-Infrastruktur. Bei diesem Geschäftsmodell werden nach einem erfolgten Angriff teilweise horrende Lösegeldforderungen gestellt, damit die Daten wieder entschlüsselt werden können. Mit fatalen Folgen: Ein Cyberangriff kann einen Betrieb in den Konkurs führen. Kleine Firmen leisten sich oft keine IT-Sicherheitsdienste und organisieren ihre eher einfachen IT-Systeme selber. Dadurch sind sie leichter angreifbar.

Ein Klick genügt

Die Melde- und Analysestelle Informationssicherung MELANI des Nationalen Zentrums für Cybersicherheit (NCSC) beobachtet eine Zunahme von Phishing-Angriffen. Das sind gefälschte E-Mails, welche die Empfänger auffordern, ihre Zugangsdaten einzugeben. Ziel dieser E-Mails ist es, an sensible Daten heranzukommen. E-Mails können auch Dokumente mit einer Schad-Software enthalten. In den vergangenen Monaten wurden beispielsweise E-Mails mit einer angeblichen Steuerrückerstattung versendet.

caractères spéciaux. Utiliser des mots de passe différents, utiliser le gestionnaire de mots de passe.
- **Installer des programmes antivirus :** Les programmes antivirus gratuits sont un bon début. Les programmes de paiement contiennent souvent une protection renforcée et des fonctions supplémentaires comme des filtres anti-spam ou des bloqueurs de publicité.
- **Droits :** L'utilisateur connecté à l'ordinateur doit avoir le moins de droits possible et les travaux de maintenance doivent se faire avec un compte administrateur séparé.

En cas de cyberattaque, il convient de porter plainte contre X auprès de la police cantonale. Ne jamais verser de rançon ! Il est aussi important de sensibiliser les collaborateurs aux dangers du Net.

Informations complémentaires :
melani.admin.ch.

Roger Waber

Interview

« Un contrôle régulier devient de plus en plus important »

En 2016, l'entreprise Gujer Landmaschinen AG a été la cible d'une cyberattaque. Renato Gujer, membre de l'Association, renseigne sur les dégâts et les conséquences.

Comment votre entreprise avait-t-elle organisé son système informatique avant l'attaque ?
Renato Gujer : Nous disposions d'un réseau propre et avons effectué quotidiennement une sauvegarde de nos données. De plus, nous avons régulièrement sauvegardé nos données sur un support externe. Le problème a révélé que le contrôle de cette gestion n'a pas été assez conséquent.

Comment s'est déroulée cette attaque ?
Les écrans sont restés figés, un des programmes a été crypté. Deux disques durs ont été détruits, parmi lesquels le disque de sauvegarde des données. En particulier la documentation et les images, tout ce que nous avions enregistré depuis la dernière sauvegarde était crypté.

Comment les attaquants se sont-ils manifestés ?
Ils nous ont contactés et ont exigé une rançon en Bitcoins. Après le paiement ils libèreraient les données. Les exigences ont toujours augmenté. Cependant nous n'avons pas cédé à leur chantage.

Comment avez-vous réagi ?
Nous avons signalé le cas à la police, qui ne nous a pas laissé beaucoup d'espoir quant à retrouver les criminels ni que ceux-ci restaureraient les données. Nous avons également envoyé les données à un soi-disant expert, qui a prétendu pouvoir éventuellement restaurer les données. Ce fut une erreur et nous avons perdu un mois supplémentaire pendant lequel nous n'avons pas pu travailler correctement.

Comment avez-vous réussi à récupérer les données ?
Nous avons dû tout reconstruire en ce qui concernait la période touchée. Par chance, nous ne nous fions pas seulement au tout électronique et avons gardé les factures et autres documents importants sur papier.

Quelle leçon avez-vous tirée de cette affaire ?
Nous avons transmis la sauvegarde des données à une société externe. Actuellement nous disposons de deux disques virtuels dans l'entreprise et en plus les données sont sauvegardées en externe. Comme nous savons maintenant qu'il peut toujours arriver que les données soient cryptées, la perte de données concerne au maximum une journée et nous sommes en mesure de travailler normalement le lendemain. En outre, nous avons conclu une assurance contre la perte de données.

Quelle conclusion tirez-vous de cet incident ?
Parfois on se berce dans une fausse sécurité, on part du principe qu'on a sécurisé les données, sans en avoir véritablement la certitude. Cela vaut la peine de revoir et de vérifier de temps en temps si les données sécurisées correspondent à l'état actuel. L'investissement en temps et financier pour l'électronique et les ordinateurs devient toujours plus important et il est capital d'effectuer une analyse complète et une vérification régulière pour s'assurer qu'on est toujours à jour. Ce qui s'est avéré précieux pendant la période où nous ne disposions pas de nos données a été le fait que nous traitons toujours rapidement les commandes de nos fournisseurs et payons rapidement nos factures. Le rapport de confiance que nous avons ainsi établi permet dans une telle situation une certaine marge de négociation pour honorer les engagements.

Um diese Rückerstattung zu erhalten, soll eine Excel-Datei geöffnet werden. Dieses Dokument darf man unter keinen Umständen öffnen. Das E-Mail sollte man sofort löschen, ohne darauf zu antworten. In den meisten Fällen lassen sich betrügerische Mails erkennen. Sie enthalten zum Beispiel eine obskure E-Mail-Adresse, Schreibfehler, unpersönliche Anschriften, zweifelhafte Anhänge, fordern zum Anklicken eines Links auf. Eine Bank würde zum Beispiel nie Kundeninformationen per Mail einholen. Verdächtige E-Mails nicht zu öffnen, ist nur eine Sicherheitsmassnahme unter anderen. Dazu gehören:

- **Sensible Daten nur über eine verschlüsselte Seite übermitteln:** Diese erkennt man daran, dass die URL mit https:// beginnt (das s steht für security).
- **Website schützen:** Firmen mit einer Website setzen sich besonderen Gefahren aus. Ein CMS (Content Management System) ist ein beliebtes Angriffsziel. Reduzieren lässt sich die Gefahr, indem man sicherstellt, dass immer die neuste Version installiert ist.
- **Regelmässiges Backup der Daten.**
- **Passwort Policy definieren:** Passwörter müssen regelmässig gewechselt werden. Starke Passwörter enthalten mindestens 12 Zeichen mit Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen. Unterschiedliche Passwörter verwenden, Passwortmanager verwenden.
- **Antivirenprogramme installieren:** Kostenlose Antivirenprogramme sind ein guter Anfang. Bezahlprogramme enthalten oft erweiterten Schutz und zusätzliche Funktionen wie Spamfilter oder Werbeblocker.
- **Berechtigungen:** Der am Computer angemeldete Benutzer sollte möglichst wenige Berechtigungen haben und Wartungsarbeiten mit einem separaten Administratoren-Konto durchführen.

Bei Cyberangriffen sollte man bei der Kantonspolizei Anzeige gegen Unbekannt erstatten. Auf keinen Fall Lösegeld zahlen! Wichtig ist auch, die Mitarbeiter zu sensibilisieren – sie sollten sich der Gefahren im Netz bewusst sein.

Weiterführende Informationen:
melani.admin.ch.

Roger Waber

Interview

«Regelmässige Überprüfung wird immer wichtiger»

Die Gujer Landmaschinen AG wurde 2016 Ziel einer Attacke von Cyber-Kriminellen. VR-Mitglied Renato Gujer gibt Auskunft über die Schäden und Auswirkungen.

Wie hatte das Unternehmen ihre IT vor dem Angriff organisiert?
Renato Gujer: Wir verfügten über ein eigenes Netzwerk und nahmen eine tägliche Datensicherung vor. Zusätzlich gab es in regelmässigen Abständen eine externe Datensicherung. Als Problem entpuppte sich, dass die Kontrolle über diese Handhabung nicht konsequent genug war.

Wie äusserte sich die Attacke?
Bildschirme waren eingefroren, eines der Programme war verschlüsselt. Zwei Laufwerke waren zerstört, darunter das Datensicherungslaufwerk. Vor allem Dokumentation und Bilder, alles was wir seit der letzten Hauptsicherung abgelegt hatten, war verschlüsselt.

Wie machten sich die Angreifer bemerkbar?
Sie meldeten sich und verlangten eine Zahlung in Bitcoin-Währung. Danach würden sie die Daten herausrücken. Die Forderungen wurden dann immer höher. Wir gingen aber nicht auf die Erpressung ein.

Wie habt ihr reagiert?
Wir meldeten den Fall bei der Polizei. Die gaben uns keine Hoffnung – weder dass sie die Täter ausfindig machen könnten noch, dass diese die Daten wiederherstellen würden. Wir haben die Daten auch einem sogenannten Experten gesendet, der sagte, dass er sie vermutlich wiederherstellen könne. Das war ein Irrtum, und wir verloren zusätzlich einen weiteren Monat, während dem wir nicht richtig arbeiten konnten.

Wie konntet ihr Daten wiederbeschaffen?
Wir mussten alles aus dem betroffenen Zeitabschnitt rekonstruieren. Zum Glück vertrauen wir nicht nur auf die Elektronik, sondern haben Rechnungen und andere wichtige Dokumente auch auf Papier abgelegt.

Welche Konsequenzen habt ihr gezogen?
Wir haben die Datensicherung an eine externe Firma weiter vergeben. Zurzeit haben wir zwei virtuelle Laufwerke im Haus und zusätzlich sind die Daten extern gespeichert. Da wir wissen, dass es immer wieder vorkommen kann, dass Daten verschlüsselt werden, betreffen die Datenverluste maximal den Tag, an dem es passiert, und wir können am folgenden Tag weiterarbeiten. Zusätzlich haben wir uns noch gegen Datenverlust versichert.

Welches Fazit zieht ihr aus dem Vorfall?
Man wiegt sich manchmal in falscher Sicherheit – man geht davon aus, dass man die Daten gesichert hat, hat aber keine wirkliche Gewissheit darüber. Es lohnt sich, die gesicherten Daten ab und zu zurückzuspielen und zu kontrollieren, ob diese dem wirklichen Stand entsprechen. Der zeitliche und finanzielle Aufwand für Elektronik und Computer wird immer grösser, umso wichtiger ist eine umsichtige Abklärung und die regelmässige Überprüfung, ob man noch auf dem richtigen Weg ist. Was sich in der Zeit, als wir ohne verfügbare Daten dastanden, als ausserordentlich wertvoll erwiesen hatte, war die Tatsache, dass wir unsere Lieferanten immer schnell bedienen und unsere Rechnungen sofort begleichen. Das Vertrauensverhältnis, das man sich dadurch schafft, gibt einem in einer solchen Situation einen gewissen Verhandlungsspielraum im Umgang mit Verpflichtungen.