CYBERSICHERHEIT – Immer öfter werden KMU zur Zielscheibe von Cyberkriminellen. Wir haben uns mit Pascal Lamia vom Nationalen Zentrum für Cybersicherheit über Prävention, Gefahren und das richtige Verhalten bei solchen Attacken unterhalten.

«Die Hacker erpressen die Opfer»

Standpunkt: *Welche Gefahren lauern im digitalen Raum auf KMU?*
Pascal Lamia: Dem Nationalen Zentrum für Cybersicherheit werden von Privatpersonen oder Unternehmen am häufigsten Betrugsversuche gemeldet. Bei KMU wird beispielsweise mittels Social Engineering versucht, Personen des Unternehmens durch Täuschung dazu zu bringen, etwas zu tun, was diese eigentlich nicht sollten, wie die Preisgabe von vertraulichen Informationen oder Freigabe von Kreditkartendaten und Passwörtern. Im Vorfeld wird beim Opfer Vertrauen aufgebaut, sodass dieses keinen Verdacht schöpft. Auch CEO-Betrug wird eingesetzt, indem eine Person der Finanzabteilung im Namen des Chefs gedrängt wird, eine wichtige Zahlung auszulösen. Neben solchen lauern aber auch auf der technischen Seite Risiken. So investieren KMU oft zu wenig in ihre IT-Sicherheit. Server werden vernachlässigt, sind veraltet und werden nicht gepatched. Über genau solche Lücken kommen dann Angreifer in die Systeme rein, stehlen und verschlüsseln Daten und erpressen anschliessend ihre Opfer.

Pascal Lami ist verantwortlich für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken. Bild: zVg

ZUR PERSON

Pascal Lamia ist Leiter der Operativen Cybersicherheit des NCSC und stv. Delegierter des Bundes für Cybersicherheit. www.ncsc.admin.ch. Das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre – NCSC) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken.

Wie viele Cyberangriffe werden dem Nationalen Zentrum für Cybersicherheit monatlich gemeldet?
Wir erhalten zwischen 1200 und 1600 Meldungen pro Monat. Bei diesen Meldungen handelt es sich jedoch nicht immer um einen Cybervorfall, bei dem ein Opfer geschädigt wurde. Oft befinden sich auch Meldungen zu Phishing-Versuchen darunter. Zu beachten gilt zudem, dass es in der Schweiz keine generelle Meldepflicht gibt und somit die Dunkelziffer entsprechend hoch sein kann.

DIE SCHWEIZ IST NICHT STÄRKER ODER SCHWÄCHER VON CYBERANGRIFFEN BETROFFEN ALS ANDERE STAATEN. GENERELL GILT NATÜRLICH, DASS JENE LÄNDER MEHR IM FOKUS VON CYBERKRIMINELLEN STEHEN, WO AUCH MEHR GELD ZU HOLEN IST.

Welche Trends können Sie aus diesen Meldungen ablesen?
Die Statistiken der eingegangenen Meldungen zeigen, dass Cyberangriffe wellenartig erfolgen. Auch festzustellen ist, dass die Angreifer sehr innovativ sind und immer neue Angriffsszenarien hervorbringen. Das NCSC berichtet wöchentlich in seinen Rückblicken auf der Website über neue Angriffsmethoden.

Ist die Schweiz von Cybercrime stärker betroffen als andere Länder?
Die Schweiz ist nicht stärker oder schwächer von Cyberangriffen betroffen als andere Staaten. Generell gilt natürlich, dass jene Länder mehr im Fokus von Cyberkriminellen stehen, wo auch mehr Geld zu holen ist.

Woher kommen die Cyberkriminellen, sind das Einzelpersonen oder organisierte Banden?
Bei Cyberkriminellen handelt es sich mehrheitlich um gut organisierte Gruppierungen mit jeweils eigenem Geschäftsmodell. Während einige eher regional organisiert sind, gibt es andere, deren Mitglieder auf der ganzen Welt verteilt sind.

Man liest immer wieder, dass die Erpressung mit gestohlenen Daten, sogenannte Ransomware-Angriffe, zunehmen. Können Sie uns erklären, was Ransomware ist?
Bei Ransomware-Angriffen handelt es sich um eine bestimmte Art einer Cyberattacke, bei der die Angreifer in fremde Systeme eindringen, Daten stehlen und diese mittels Verschlüsselungssoftware verschlüsseln. Sind Daten einmal verschlüsselt, können sie nur mit dem passenden Schlüssel wieder geöffnet werden. Die Hacker erpressen die Opfer damit, den Schlüssel gebe es nur nach Bezahlung des Lösegelds. In neueren Varianten wird zudem gedroht, die gestohlenen Daten zu veröffentlichen, falls kein Lösegeld bezahlt wird.

Wie ist der Anstieg von solchen Attacken zu erklären?
Ransomware-Angriffe können sich je nach Höhe des Lösegeldes für die Täter als lukrative Geldquelle erweisen. Jede erfolgreiche Erpressung motiviert die Angreifer zum Weitermachen, finanziert die Weiterentwicklung der Angriffe und fördert deren Verbreitung. Deshalb rät das NCSC klar von der Zahlung eines Lösegeldes ab.

Wie soll man sich verhalten, wenn man als Firma oder Behörde gehackt und sogar erpresst wird?
Das NCSC empfiehlt generell bei Cybervorfällen, die zuständigen Polizeibehörden sowie das NCSC zu kontaktieren und jeweils transparent, ehrlich und offen zu kommunizieren. Unternehmen sollten es aber gar nicht erst darauf ankommen lassen. Sie sollten sich auf Cyberangriffe vorbereiten und die dringend nötigen Vorkehrungen treffen. Dazu gehören das Einhalten des Grundschutzes wie Virenschutz, Firewall, regelmässiges Updaten der Hard- und Software und das regelmässige Speichern der Daten auf einem externen Datenspeicher.

Auch die Sensibilisierung der Mitarbeitenden ist ein wichtiger Faktor. Ausserdem sollte auch ein Business-Continuity-Plan und ein Krisen-Kommunikationskonzept erstellt werden.

IM HOMEOFFICE VERMISCHT SICH DAS PRIVAT- UND DAS ARBEITSLEBEN, WAS AUCH AUSWIRKUNGEN AUF DIE CYBERSICHERHEIT HAT.

Opfer von Cybercrime sind alle Arten von KMU und Behörden: Gemeinden, Hersteller von Sonnen- und Wetterschutz, Kantonalbanken, Hersteller von Verbindungstechnik, Uhrenhersteller, Privatkliniken, Medienhäuser. Nach welchem Prinzip werden die Firmen von den Kriminellen «ausgesucht»?
Im Fokus der Angreifer stehen alle verwundbaren Systeme, unabhängig, ob es sich um kleine oder grosse Unternehmen oder Behörden handelt. Sind Systeme gut geschützt, ist das Eindringen für Angreifer viel schwieriger und aufwändiger. Grössere Unternehmen oder Behörden sind betreffend IT-Sicherheit oftmals besser aufgestellt, da sie über mehr Ressourcen verfügen.

Gibt es Branchen, die mehr gefährdet sind als andere?
Hier gilt es nicht nach Branchen zu unterscheiden, sondern danach, wie stark ein Unternehmen digitalisiert ist.

Was bedeutet der Trend zu Homeoffice für die Cybersicherheit eines Unternehmens?
Im Homeoffice vermischt sich das Privat- und das Arbeitsleben, was auch Auswirkungen auf die Cybersicherheit hat. Oft werden daheim die Computer sowohl für Privates als auch Berufliches verwendet. Dies kann zu Sicherheitslücken führen, wodurch Cyberkriminelle die Firma angreifen können. Deshalb sollte man entweder berufliche und private Geräte trennen oder der Arbeitgeber richtet einen sicheren Zugang auf die Firmen-IT-Infrastruktur ein.

DA ALLE VERWUNDBAREN SYSTEME FÜR CYBERKRIMINELLE INTERESSANT SIND, MUSS SICH JEDES UNTERNEHMEN UND JEDE BEHÖRDE GEDANKEN ZUR CYBERSICHERHEIT MACHEN.

Wie stark muss sich auch eine Schlosserei mit 12 Angestellten oder ein freiberuflicher Treuhänder Gedanken über seine Cybersicherheit machen?
Da alle verwundbaren Systeme für Cyberkriminelle interessant sind, muss sich jedes Unternehmen und jede Behörde Gedanken zur Cybersicherheit machen. Cybersicherheit ist wichtig und somit «Chefsache».

Was können KMU – speziell auch mittlere und kleine Unternehmen – im Bereich Cybersicherheit tun?
Wesentlich ist, dass die Unternehmen der Cybersicherheit genügend Bedeutung beimessen. Die Zuständigkeit muss hier klar geregelt sein. Dies kann entweder durch interne Sicherheitsspezialisten sichergestellt oder kann auch an externe Firmen ausgelagert werden. Ungeachtet, welche Lösung zum Zug kommt, die Verantwortung für die Cybersicherheit bleibt Aufgabe des Unternehmens oder der Behörde.

Interview: Patrick Herr

SCHÜTZEN SIE IHRE KONTEN UND PASSWÖRTER

Sowohl Ihr Rechner und Ihr Mobiltelefon als auch unterschiedliche Online-Dienste verlangen die Vergabe eines Passwortes. Schlecht gewählte oder zu kurze Passwörter stellen ein erhebliches Sicherheitsrisiko dar. Schützen Sie Ihre Geräte und Online-Zugänge vor fremdem Zugriff, so wie Sie die Türe abschliessen, wenn Sie das Haus oder die Wohnung verlassen.

Passwort nicht mehrfach verwenden
Verwenden Sie für jeden einzelnen Online-Dienst ein anderes Passwort.

Aktivieren Sie nach Möglichkeit die sogenannte Zwei-Faktor-Authentifizierung
Schützen Sie den Zugang zu Ihren Internetdiensten falls verfügbar mit einer Zwei-Faktor-Authentifizierung (Einmal-Passwort, SMS-Token usw.).

Mindestlänge von 12 Zeichen
Die Mindestlänge des Passwortes sollte bei 12 Zeichen liegen und aus Klein- und Gross-Buchstaben, Zahlen und Sonderzeichen bestehen.

Passwort ändern
Bei Firmen muss sichergestellt sein, dass unpersönliche Passwörter geändert werden, wenn Mitarbeitende die Firma verlassen. Optional wird empfohlen, Zyklen zum Ändern von Passwörtern zu definieren.

Passwortmanager
Passwortmanager sind Programme zum Verwalten der verschiedenen Passwörter, die von Benutzenden eingesetzt werden. Der Zugang zum Passwortmanager ist durch ein «Master-Passwort» geschützt. Setzen Sie am besten einen Passwortmanager ein, der eine sogenannte «Zweifaktoren-Authentisierung» unterstützt. Ist das nicht der Fall, muss das Masterpasswort sehr stark sein: Wird es entwendet, erhalten Unbefugte Zugang zu allen im Passwortmanager gespeicherten Passwörtern.

Lassen Sie sich nicht über die Schulter schauen
Wenn Sie Notebooks und mobile Geräte in der Öffentlichkeit verwenden, benutzen Sie einen Sichtschutz. Spezielle Folien können Sie im Fachhandel erwerben. Sperren Sie den Bildschirm, wenn Sie nicht aktiv am Gerät arbeiten. Lassen Sie die Geräte nie unbeaufsichtigt an öffentlichen Orten, sondern tragen Sie diese auf sich.

Vorsicht bei der Passworteingabe
Geben Sie niemals ein Passwort auf einer Seite an, welche Sie über einen Link geöffnet haben. Geben Sie immer die Adresse (URL) zum entsprechenden Online-Dienst manuell in der Adresszeile Ihres Browsers ein.

Geben Sie das Passwort nie heraus
Finanzinstitute, Telekommunikations- und sonstige Dienstleistungsunternehmen fragen nie nach einem Passwort (weder per E-Mail noch per Telefon) und verlangen auf diese Weise auch keinen Passwortwechsel.

(Quelle: www.ncsc.admin.ch)