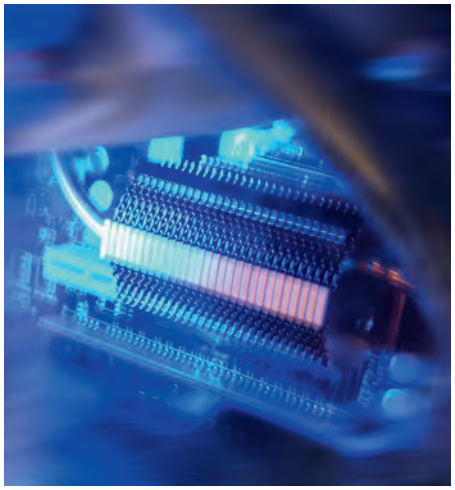

Protection Fa
Safety Compromised

Den Cyberkriminellen einen Schritt voraus

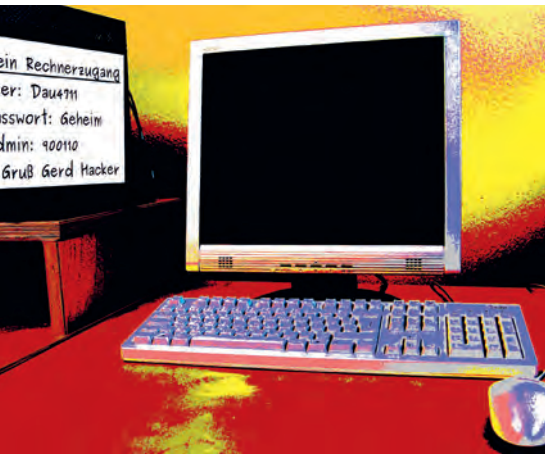
Text **Tobias Ellenberger**

KMU werden zu einem immer beliebteren Ziel von Cyberangriffen. Ist ein Unternehmen einer solchen Situation völlig unvorbereitet ausgesetzt, kann dies verheerende Auswirkungen haben. Umso wichtiger ist es, dass auch KMU im Rahmen ihrer Möglichkeiten für ein Mindestmass an IT-Sicherheit sorgen, um sich gegen die häufigsten Arten von Angriffen zu rüsten.



Gegen Angriffe aus der Tiefe des Internets müssen sich nicht nur Grossbetriebe wappnen. (Bild rechts: IStock, Bild oben: Rainer Sturm / Pixelio)

Autor Tobias Elleneberger ist Chief Operating Officer und Vice Chairman der Oneconsult AG und Vizepräsident von Swiss Cyber Experts.



So nicht! Zugangsdaten müssen an einem sicheren Ort aufbewahrt werden. (Bild: Rudolpho Duba / Pixelio)

Längst sind Cyberangriffe nicht mehr nur ein Thema für grosse Unternehmen, in denen Cyberkriminelle vermeintlich reiche Beute machen können. KMU rücken immer mehr in den Fokus von Angreifern. Während früher vor allem Banken ein interessantes Ziel waren, bleiben heute alle Branchen und auch kleine Handwerksbetriebe nicht verschont.

125 von 503 befragten KMU, das sind 25 Prozent, gaben in einer im Oktober 2020 durchgeführten Studie von ICTSwitzerland an, schon einmal erfolgreich angegriffen worden zu sein. Zu den häufigsten Angriffsmethoden zählen allgemein Schadsoftware (auch als Malware bekannt, zum Beispiel Viren oder Trojaner) und Phishing.

Letztere Methode nutzen Angreifer, um mithilfe gefälschter E-Mails oder Websites an persönliche Daten wie Kontoinformationen oder Passwörter zu gelangen oder Benutzer dazu zu bewegen, eine für sie selber schädliche Aktion durchzuführen.

Die Methode

Besonders verbreitet sind derzeit Angriffe mit einer speziellen Form von Schadsoftware, einer Ransomware (engl. *ransom* = Lösegeld). Angreifer setzen diese ein, um sämtliche Daten eines Unternehmens zu entwenden, anschliessend zu verschlüsseln und dann per Droh-E-Mail ein Lösegeld zu erpressen, gegen dessen Bezahlung die Daten angeblich wieder entschlüsselt werden.

So erging es einem Schweizer Familienunternehmen aus dem Handwerk, das durch einen solchen Angriff mehrere Tage lang komplett lahmgelegt wurde. Die Angreifer forderten ein Lösegeld in Höhe von 270 000 Dollar, anderenfalls würden sie, so die Drohung, dem Unternehmen höchstmöglichen Schaden zufügen.

Das Unternehmen kam in diesem Fall mit einem blauen Auge davon, da es gut vorbereitet war und zeitnah die richtigen Experten kontaktierte, anstatt auf die Forderung der Angreifer einzugehen.

Die Hintergründe

Ein wichtiger Faktor für den grossen Erfolg solcher Angriffe gerade bei KMU ist das fehlende Bewusstsein dafür, welche schwerwiegenden Folgen eine Cyberattacke haben kann. Sie kann dazu führen, dass geschäftskritische Systeme und Daten – zum Beispiel Terminkalender, Kontakte und Kundendaten – tagelang nicht verfügbar sind, was einen mehrtägigen Unterbruch des Geschäftsbetriebs nach sich zieht.

Hinzu kommen in vielen Fällen hohe Kosten für die Wiederherstellung des Normalbetriebs. Eine Garantie, dass der Ursprungszustand wiederhergestellt werden kann, gibt es in keinem Fall.

Kleine besonders gefährdet

Für kleine Unternehmen können die Auswirkungen eines derartigen Vorfalls existenzgefährdend sein. Der Schaden beschränkt sich dabei nicht nur auf das

Finanzielle. Auch die Reputation und damit das Vertrauen der Kunden werden oft in Mitleidenschaft gezogen.

Die Vorbereitung

Deshalb müssen auch KMU, die in der Regel nicht über eigene Cyber-Security-Ressourcen verfügen, Massnahmen umsetzen, um sich im Rahmen ihrer Möglichkeiten bestmöglich gegen Cyberangriffe zu schützen und dafür vorbereitet zu sein.

Das wirksamste Schutzmittel stellt nach wie vor die Prävention dar. Dabei ist es wichtig zu berücksichtigen, dass Prävention ein laufender Prozess und keine einmalige Aktivität ist. So reicht es offensichtlich nicht aus, Updates einmalig zu installieren, sondern die Massnahmen müssen regelmässig durchgeführt und überwacht werden.

Fremde Hilfe reicht nicht

Die meisten KMU geben ihre IT in die Hände eines Dienstleisters. Dies sollte jedoch nicht zum Trugschluss führen, dass es damit nicht mehr notwendig ist, sich selbst mit dem Thema Cybersicherheit zu beschäftigen. KMU sollten selber gewisse Vorkehrungen treffen und bei der Auswahl eines Dienstleisters prüfen, welche Fähigkeiten dieser im Hinblick auf IT-Sicherheit mitbringt.

Während der Zusammenarbeit sollten Unternehmen in aktivem regelmässigem Austausch mit ihrem IT-Dienstleister darüber sprechen, was im Moment relevant und aktuell ist. So ist es ratsam, sich beispielsweise alle drei bis sechs Monate über mögliche Schwierigkeiten mit der IT-Sicherheit und den daraus entstehenden Handlungsbedarf auszutauschen. Dies stellt sicher, dass der Sicherheitsaspekt laufend beachtet wird.

Provider sorgfältig wählen

Auch bei der Auswahl anderer Provider, beispielweise Cloud-Provider, sollte die Frage, wie das Thema Sicherheit beim jeweiligen Anbieter gehandhabt wird, unbedingt in die Entscheidung einfliessen. In der Regel können grosse Cloud-Betreiber mehr in die Sicherheit investieren und somit sicherere Lösungen anbieten. Wirklich geschützt sind die Daten aber erst dann, wenn auch beim Endnutzer weitere Sicherheitsmassnahmen getroffen werden.

Grundsätzlich gilt es für ein KMU, zunächst abzuwägen, wie viel in die Cybersicherheit investiert werden kann und welche Massnahmen in diesem Rahmen am sinnvollsten und effizientesten sind.

Investitionen sollten immer in Relation dazu gesetzt werden, was damit erreicht werden kann. Es ist nicht sinnvoll, blind Unmengen in die IT-Sicherheit zu investieren – insbesondere, wenn das Budget begrenzt ist – und irrtümlicherweise davon auszugehen, dass damit ein 100-prozentiger Schutz gegen Cyberangriffe gewährleistet ist. Vielmehr sollten KMU mit ihrem verfügbaren Budget gezielt angemessene Vorkehrungen für Prävention und Abwehr treffen. Hierfür ist es hilfreich und empfehlenswert, sich regelmässig damit auseinander zusetzen, welche Angriffsarten gerade stark verbreitet sind. Eine nützliche Quelle ist beispielsweise der wöchentliche Newsletter des Nationalen Zentrums für Cybersicherheit (NCSC), in dem zusammenfassend über die wichtigsten Vorkommnisse berichtet wird.

Auch lohnt sich ein regelmässiger Blick auf die Website des NCSC, das dort Meldungen zu kritischen Schwachstellen oder gehäuften Angriffen herausgibt. Über grossflächig angelegte Angriffe berichten zudem auch Tageszeitungen oder die Nachrichten in TV und Radio.

Fernzugriff schützen

Geht man nun zu konkreten technischen Massnahmen über, sollten KMU mit ihrem IT-Dienstleister zunächst unbedingt klären, wie der Fernzugriff auf das Unternehmensnetzwerk geschützt ist. Dabei ist zu berücksichtigen, dass nicht nur die

Cyber-Security-Dienstleistungen

Die Oneconsult AG mit Hauptsitz in Thalwil ZH und Niederlassungen in Bern und München (D) bietet verschiedene Dienstleistungen im Bereich Cybersicherheit an, darunter Beratungsservices und simulierte Hackerangriffe als Tests. Die Firma begleitet regelmässig Unternehmen bei der Bewältigung von Ransomware und vergleichbaren Angriffen.

Mitarbeitenden von extern darauf zugreifen können, sondern auch Partner des Unternehmens wie etwa Treuhänder. Die gängigste Methode für den sicheren Zugriff ist ein Virtual Private Network (VPN). Doch werden keine zusätzlichen Sicherheitsmassnahmen umgesetzt, sind auch über einen geschützten VPN-Tunnel Angriffe möglich. Daher sollte mit relevanten Partnern und Lieferanten abgesprochen werden, wie diese das Thema Cybersicherheit handhaben. Dazu gehört, von diesen ein bestimmtes Mass an Vorkehrungen einzufordern, damit sie nicht zum Einfallstor für Angriffe auf das eigene Unternehmen werden.

Die grundlegenden Massnahmen

Nachfolgend sind grundlegende Massnahmen beschrieben, die KMU umsetzen sollten, um ein Mindestmass an IT-Sicherheit zu gewährleisten und sich gegen die gängigsten Arten von Cyberangriffen zu schützen. Die Reihenfolge der einzelnen Massnahmen ist nicht als Priorisierung zu verstehen.

1. Antiviren-Software

Auf sämtlichen Systemen sollte eine aktuelle Antiviren-Software installiert werden zum Schutz gegen Viren, Spam, Ransomware usw. Mit der Installation einer solchen Software allein ist es jedoch noch nicht getan. Die Antiviren-Lösung muss stets aktiviert sein und regelmässig aktualisiert werden.

Des Weiteren müssen die Verantwortlichen die Warn- und Fehlermeldungen, welche die Software ausgibt, aktiv überwachen und verarbeiten. Eine Antiviren-Software kann Bedrohungen zwar erkennen, ist aber nicht immer in der Lage, diese auch unmittelbar und ohne weiteres Zutun zu beseitigen. Eine Antiviren-Lösung stellt somit erst dann einen effizienten Schutz dar, wenn sie stets auf dem aktuellen Stand ist und aktiv überwacht wird.

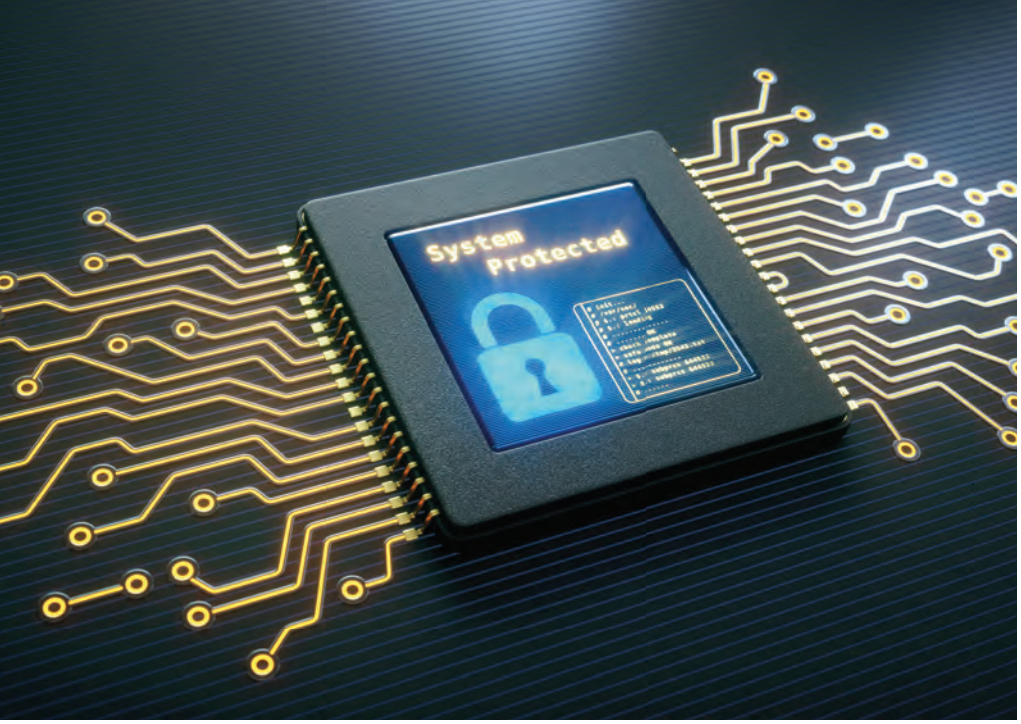
2. Firewall

Eine weitere Massnahme ist die Installation einer Firewall, um Systeme vor unerlaubten Zugriffen zu schützen. Eine Firewall überwacht den eingehenden und ausgehenden Netzwerkverkehr und erlaubt beziehungsweise blockiert diesen entsprechend. Sie bildet die erste Verteidigungslinie. Wie auch für die Antiviren-Lösung gilt hier,

Leitfäden und Checklisten

Einen detaillierten Leitfaden zum Thema Cybersicherheit für KMU finden Sie zum Beispiel auf der Webseite von ICTSwitzerland. Die Global Cyber Alliance bietet ausserdem ein «Cybersecurity Toolkit» für KMU an, das Schutzmassnahmen sowie kostenlose Tools zur Umsetzung umfasst.
Ein Schnellcheck zur Cybersicherheit lässt sich durchführen unter:

digitalswitzerland.com/de/kmu-schnell-check/



25 Prozent der KMU gaben in einer Befragung an, Cyberkriminelle hätten schon einmal mit einem Angriff auf sie Erfolg gehabt. (Bild: IStock)

dass sie stets auf dem aktuellen Stand gehalten werden muss und Meldungen zu überwachen sind.

Eine Firewall sollte die Schutzmauer des Unternehmens gegenüber dem Internet sein (Perimeter-Firewall). Sie sollte aber auch auf den Computern zusätzlich zum Antivirenprogramm aktiv sein, um allfällige «interne» Schadprogramme abwehren zu können, die beispielsweise über ein Speichermedium ins Netzwerk gelangen.

3. Regelmässige Updates

Sämtliche verwendete Software ist regelmässig zu aktualisieren und stets auf dem aktuellen Stand zu halten. Dies gilt für sämtliche im Unternehmen verwendeten Systeme und Geräte. Eventuelle Sicherheitslücken lassen sich dadurch zeitnah schliessen und bieten somit keine Angriffsfläche. Um sicherzustellen, dass bei der regelmässigen Installation von Updates keine Komponente übersehen wird, ist zunächst eine Bestandsaufnahme sämtlicher Software und Hardware nötig. Wo möglich, sollten automatische Updates aktiviert sein.

Geräte oder Software, für die keine Updates mehr verfügbar sind, sind wenn immer möglich umgehend ausser Betrieb zu nehmen und zu isolieren. Ausserdem empfiehlt es sich, in regelmässigen Abständen, beispielsweise einmal wöchentlich, zu prüfen, ob alle Geräte auf dem aktuellen Stand sind. Dies umfasst nicht nur die PCs vor Ort, sondern auch Smartphones und Notebooks von Mitarbeitenden. Am besten ist im Betrieb eine Person für das Aktuellhalten sämtlicher technischer Geräte verantwortlich und erhält Zeit dafür zugesprochen.

4. Back-ups

Ein weiterer Schritt ist die regelmässige Sicherung aller Geschäftsdaten. Damit diese im Ernstfall ihren Zweck erfüllt und zur Wiederherstellung der Daten genutzt werden kann, gilt es, bei der Backup-Erstellung einige wichtige Punkte zu berücksichtigen: Zum einen sollte vorab sichergestellt sein, dass das Back-up auch wirklich wie vorgesehen funktioniert und ausreichend Daten sichert. Zum anderen sollte die Sicherung so aufbewahrt werden, dass sie bei einem Systemausfall verfügbar ist, das bedeutet getrennt vom Unternehmensnetzwerk (offline zum Beispiel auf einer externen Festplatte) und an einem externen, geschützten Ort.

Rechnen Sie damit, dass ein Angreifer aktiv versuchen wird, Ihre Back-ups zu löschen, um Ihnen einen möglichst hohen Schaden zuzufügen! Diese Überlegung muss in die Planung des Back-up-Konzepts einfliessen.

5. Schulung aller Mitarbeitenden

Die Mitarbeitenden sind regelmässig im Umgang mit E-Mails, dem Internet sowie vorhandenen IT-Systemen und Daten zu schulen und auf mögliche Gefahren sowie Risiken zu sensibilisieren. Dazu gehört unter anderem, ein gesundes Misstrauen gegenüber unerwarteten E-Mails zu hegen, nicht unüberlegt auf Links oder Dateianhänge zu klicken oder Firmendaten niemals über private Kanäle weiterzuleiten. Solche Schulungen haben kontinuierlich stattzufinden. Am besten werden dabei aktuelle Ereignisse und Gefahren einbezogen.

Es sollten niemals sensible Daten wie Angaben zu Umsätzen oder Kundenlisten öffentlich auf der Unternehmenswebsite einsehbar sein. Personen, zu denen in öffentlich verfügbaren Quellen Daten gefunden werden können, sind oft das Einfallstor für Angriffe. Und es erleichtert Kriminellen, das Vertrauen von Mitarbeitenden zu erschleichen, wenn sie über konkrete Informationen zum Unternehmen verfügen. Umsatzzahlen können zudem ein Hinweis sein, ob sich eine Attacke lohnt.

Genauso können Mitarbeitende aber – bei richtiger Schulung und Sensibilisierung – die Chance bieten, Angriffe zu erkennen, die durch technische Hilfsmittel unentdeckt bleiben würden, so zum Beispiel beim sogenannten CEO Fraud (engl. *CEO* = Geschäftsführer, engl. *fraud* = Betrug). Bei dieser Methode versucht ein Angreifer, unter Vorgabe einer falschen Identität (häufig eines Mitglieds der Unternehmensleitung) mit einem gefälschten E-Mail den Empfänger (eine Mitarbeitende oder einen Mitarbeitenden) dazu zu bewegen, eine Überweisung an den im E-Mail genannten Kontakt zu tätigen. →

Wer bei einem Angriff nicht in grosse Schwierigkeiten geraten möchte, sollte einen Notfallplan erstellen.

Solche E-Mails erscheinen auf den ersten Blick meistens nicht ungewöhnlich und sie weichen oft nur im Detail – jedoch in entscheidenden Teilen – von legitimen E-Mails ab. Nur der Empfänger oder die Empfängerin des E-Mails kann erkennen, dass unter anderem die Bankverbindung nicht mit den korrekten Daten übereinstimmt, und so den Angriffsversuch identifizieren. Ein automatischer Mechanismus würde dies nicht erkennen.

6. Benutzerverwaltung

Alle Mitarbeitenden haben auf sämtliche Daten und Anwendungen vollen Zugriff, damit diese auf allen Ebenen schnell und einfach verfügbar sind. Das klingt zunächst praktisch, sollte aber keinesfalls in dieser Form zutreffen! Benutzer sollten jeweils nur die Zugriffsrechte bekommen, die sie wirklich benötigen. Diese sollten basierend auf Rollen wie Geschäftsführung, Sekretariat, Aussendienst, Finanzen usw. vergeben werden.

Ausserdem müssen alle Benutzer über ein eigenes persönliches Konto verfügen. Es sollten keine gemeinsamen Benutzerkonten im Einsatz sein. Wenn Mitarbeitende das Unternehmen verlassen, sollten die Zugriffsrechte entsprechend entzogen und das Benutzerkonto gesperrt werden.

Mithilfe einer Benutzerverwaltung lässt sich verhindern, dass ein Angreifer Zugriff auf sämtliche Informationen und Systeme erlangt, wenn er sich beispielsweise erfolgreich Zugang zum Konto von einzelnen Mitarbeitenden verschafft.

7. Starke Passwörter

Nur starke Passwörter schützen Geräte und Benutzerkonten gut. Sichere Passwörter sind nur sicher, wenn sie nicht für mehrere Konten verwendet werden. Und sie sind ausreichend lang (zum Beispiel mindestens zwölf Zeichen für normale Mitarbeiterkonten ohne besondere Berechtigungen). Im Idealfall besteht ein Passwort aus einem vollständigen, selbst ausgedachten Satz inklusive Satzzeichen. Mitarbeitende sollten auch im Umgang mit Passwörtern geschult werden.

Um darüber hinaus zusätzliche Sicherheit zu bieten, kann der Einsatz einer 2-Faktor-Authentisierung (2FA) in Betracht gezogen werden.

8. Notfallplan

Damit die notwendigen Schritte im Ernstfall klar sind, ist vorab ein Notfallplan zu erstellen. Ein solcher Plan umfasst vor allem kritische Systeme und Daten, relevante Kontaktpersonen sowie Massnahmen zur Reaktion auf einen Cyberangriff. Es empfiehlt sich, dieses Szenario einmal durchzuspielen, damit Ablauf und Zuständigkeiten bekannt sind und gegebenenfalls Anpassungen vorgenommen werden können. Dabei sollte auch bedacht werden, dass elektronische Systeme möglicherweise nicht mehr zur Verfügung stehen, Der Notfallplan sollte also in zugänglicher Form (zum Beispiel als

Ausdruck) an einem sicheren Ort verwahrt sein. Eine durchdachte und zeitnahe Reaktion ist bei einem Angriff ausschlaggebend, um Schlimmeres zu verhindern.

Das Fazit

Wie bereits eingangs erwähnt und wie auch aus den aufgeführten Massnahmen deutlich wird, stellt eine solide Vorbereitung das wirksamste Schutzmittel gegen Cyberangriffe dar. Es ist daher empfehlenswert, sich nicht erst im Ernstfall, sondern bereits im Vorfeld mit dem Thema auseinanderzusetzen und gegebenenfalls einen Experten in diesem Bereich zu kontaktieren.

Dies bietet Unternehmerinnen und Unternehmern die Chance, sich mit fachkundiger Unterstützung auf mögliche Szenarien vorzubereiten, sodass im Ernstfall durch eine schnelle und angemessene Reaktion Schlimmeres verhindert werden kann.

Wenn KMU die beschriebenen grundlegenden Massnahmen, die im Kern aus Prävention, Wartung und Reaktion bestehen, sorgfältig umsetzen, können sie den Cyberkriminellen einen Schritt voraus sein.