So rüsten sich KMU

Cyberrisiken Mit minimalen Standards bei IT-Sicherheit können sich Unternehmen viel Ärger und hohe Kosten sparen. Doch Sicherheit ist ein Prozess, kein Zustand.

GIOIA DA SILVA

Mit dem Abarbeiten einer Checkliste ist es nicht getan», warnt Matthias Bossardt, Partner bei KMPG und Leiter der Cybersicherheitsabteilung. Informationssicherheit müsse sich stetig weiterentwickeln und sich der Bedrohungslage anpassen. «Checklisten helfen aber vielen Unternehmen, keinen wichtigen Aspekt aus den Augen zu verlieren und einen Minimalstandard an Cybersicherheit aufrechtzuerhalten. So können sich Unternehmen viele der täglichen Angriffe aus dem Netz vom Leib halten.»

Verschiedene Beratungsunternehmen und öffentliche Stellen haben Leitfäden und Checklisten speziell für KMU entwickelt, wie solche Mindeststandards erreicht werden können. Bei folgenden Punkten überschneiden sich die Empfehlungen:

1. Wen interessierts? Bestimmen Sie Personen, die sich um Cybersicherheitsanliegen kümmern und erstellen Sie ein Pflichtenheft für die IT-Verantwortlichen. Verteilen Sie das Know-how am besten auf mehrere Personen.

2. Weiterbildung: Die meisten Cyberattacken geschehen über Phishing-E-Mails. Sensibilisieren Sie Ihre Belegschaft mit Informations- und Ausbildungskampagnen auf Cyberrisiken. Richten Sie eine niederschwellige Anlaufstelle ein, wo Mitarbeitende Cyberbedenken melden können. Kommunizieren Sie offen, dass sich niemand dafür schämen muss, falls er oder sie auf eine Phishing-Mail reinfällt. Wichtig ist, dass schnell gehandelt wird.

3. Kronjuwelen: Schützen Sie den Kernbereich Ihres Unternehmens besonders gut. Definieren Sie Kronjuwelen und stellen Sie ein Konzept auf, wie Sie diese besonders sicher halten.

4. Schatten-IT: Erstellen Sie ein Inventar von IT-Systemen und Geräten, die in Ihrem Unternehmen eingesetzt werden. Benützen Sie keine Schatten-IT, zum Beispiel Gratissysteme zum Datenaustausch oder -versand, die nicht in Ihre Sicherheitsarchitektur eingebunden sind. Definieren Sie Regeln, falls Sie eine «bring your own device»-Kultur leben.

5. Eintrittspforte durch das Internet der Dinge? Prüfen Sie Geräte und Objekte, die mit dem Internet der Dinge verbunden sind oder mit Drittpersonen kommunizieren.

6. Mobile Geräte: Verschlüsseln Sie mobile Datenträger wie Smartphones, schützen Sie sie mit einem Passwort und benützen Sie keine öffentlichen WLAN-Hotspots. Prüfen Sie, welche Apps Zugriff auf Daten auf dem Telefon bekommen und hinterfragen Sie, ob dies wirklich nötig ist.

7. Zugangsmechanismen: Prüfen Sie Zugangsmechanismen, wählen Sie starke Passwörter und führen Sie die Zwei-Faktor-Authentifizierung ein.

8. Virenschutz: Investieren Sie in gute Virenschutzprogramme und schützen Sie Ihren Internetzugang mit einer Firewall. Aktivieren Sie die automatischen Softwareaktualisierungen oder stellen Sie sicher, dass regelmässige Updates durchgeführt werden.

9. Segmentierung: Definieren Sie, wer Zugriff auf welche Systeme und Datenablagen benötigt. Prüfen Sie Administratorenrechte und überwachen Sie die Segmentierung.

10. Hacken Sie sich selbst: Führen Sie regelmässige Sicherheitstests durch und scannen Sie ihre Systeme auf unerwünschte Elemente. Penetration Tests von externen, gutmütigen Hackern können helfen, die Belegschaft für das Thema Cybersicherheit zu sensibilisieren und Sicherheitslücken zu entdecken (siehe Text unten).

11. Backup: Erstellen Sie regelmässig Sicherungskopien Ihrer Daten.

12. Vorbereitung auf den Ernstfall: Erarbeiten Sie ein Notfallkonzept und üben Sie hin und wieder den Ernstfall.

13. Melden Sie schwerwiegende Vorfälle: Die Melde- und Analysestelle Informationssicherung des Bundes (Melani) koordiniert Massnahmen zur Cyberabwehr und führt ein Frühwarnsystem. Ausserdem berät die Stelle betroffenen Firmen. Melden Sie schwerwiegende Vorfälle unter www.melani.admin.ch.

SCHNELLTESTS

Ein erster Check für KMU

Fragen Ist eine Person für die Cybersicherheit zuständig? Nutzen Sie die Möglichkeit der automatischen Softwareaktualisierung? Existieren betriebliche Richtlinien und Weiterbildungen zum sicheren Umgang mit E-Mails, digitalen Daten und dem Internet?

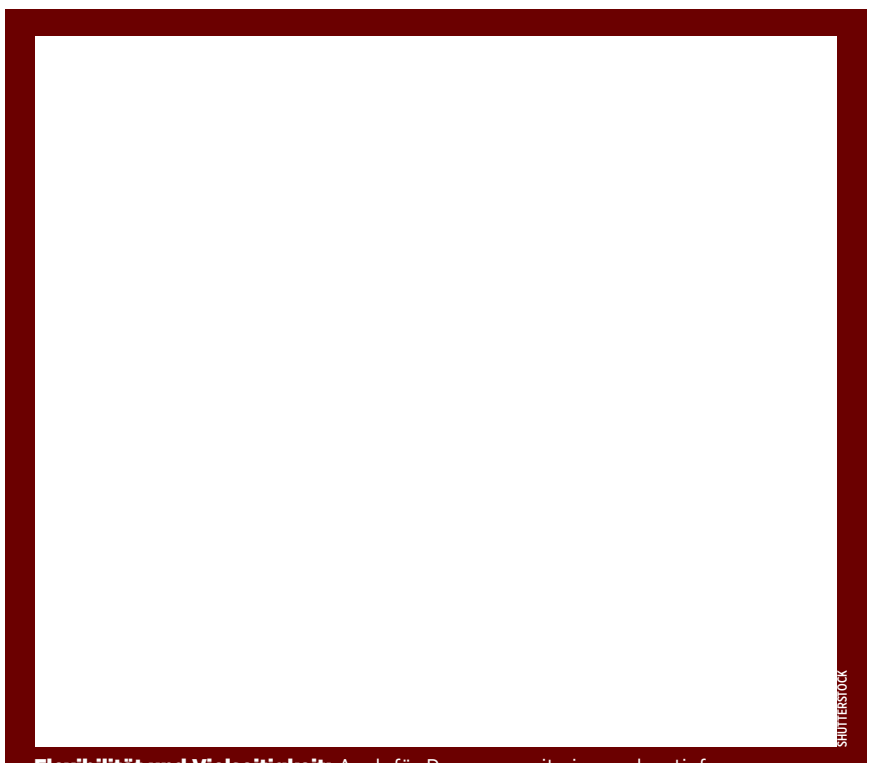
Link Der Online-Schnelltest unter www.cybersecurity-check.ch bietet speziell für kleinere Unternehmen eine Hilfestellung, um innerhalb von wenigen Minuten herauszufinden, welche Minimalstandards dringend angegangen werden müssen.

CLOUD-DIENSTE

Unter Umständen sicherer als lokale Systeme

Angriffswellen «Viele Firmen haben Bedenken, ihre Daten in eine Cloud-Lösung auszulagern. In vielen Fällen ist die Cloud aber sicherer als mit ungenügendem IT-Sicherheitswissen betriebene, eigene Systeme», sagt Martin Leuthold, Geschäftsleitungsmitglied von Switch. Litt Microsoft, die grösste Cloud-Plattformbetreiberin, 2014 unter 20 000 Angriffen pro Woche, sind es heute zwischen 600 000 und 700 000 pro Tag. Deshalb investiert das Softwareunternehmen nach eigenen Angaben heute rund 1 Milliarde Dollar in die Sicherheit seiner Systeme. Firmen, die sich keine laufend aktualisierbaren Systeme finanzieren können, tun also unter Umständen gut daran, sich in die Cloud-Lösung eines starken Technologiepartners einzukaufen.

Restrisiko Dennoch ist auch bei der Cloud Vorsicht geboten. Schliesslich kann ein Technologiepartner, der eine Cloud-Lösung verkauft, genauso angegriffen werden wie die Cloud-Betreiberin selbst. Ausserdem ergibt sich bei der Cloud ein Klumpenrisiko: Da viele Daten und Systeme an einer zentralen Stelle gespeichert werden, ist die Cloud für Angreifer ein besonders attraktives Ziel.



SHUTTERSTOCK

Flexibilität und Vielseitigkeit: Auch für Personen mit einem eher tiefen Ausbildungsniveau, die aber handwerklich begabt sind und über hohe motorische Kompetenzen verfügen, gibt es gute Zukunftschancen.

FACHKRÄFTEMANGEL

Gute Arbeitsbedingungen schaffen

Mangel Der Verband ICT-Berufsbildung Schweiz prognostiziert, dass in der Schweiz bis im Jahr 2026 rund 40 000 IT-Fachkräfte fehlen werden. Vor allem kleinere Unternehmen fern von grossen Stadtzentren gehen im Kampf um die besten Talente oft leer aus.

Attraktivität IT-Spezialisten sind gefragte Arbeitskräfte – und das wissen sie auch. Entsprechend attraktiv sind die Arbeitsbedingungen in der Branche. Ein hohes Salär ist wichtig, aber nicht der einzige Faktor bei der Wahl des Arbeitsplatzes. Am wichtigsten sind den IT-Expertinnen und -Experten laut einer Umfrage der Beratungsfirma Universum flexible Arbeitsbedingungen. Wer ein attraktives Umfeld mit flexiblen Arbeitszeiten und Homeoffice schafft, kann Fachkräfte eher halten und wird einen besseren Schutz erreichen. Cybersicherheit endet schliesslich nicht um 17 Uhr.

ANZEIGE

Firmen hacken sich selbst

Penetration Hacker Sie versuchen, in die Firmen-IT einzudringen. Sie verhalten sich dabei ähnlich wie bösartige Hacker, jedoch mit einem anderen Ziel.

JONATHAN NOACK

«Viele Unternehmen haben ähnliche Schwachstellen», sagt Cyrill Brunschwiler, Managing Director bei Compass Security in Zürich. Seine Firma ist auf Penetration Tests spezialisiert. «Man überlegt sich, welche Person in einem Unternehmen Zugriff auf sensible Daten oder Systeme hat. Dieser Person sendet man eine E-Mail mit einer infizierten Word- oder Excel-Datei. Sobald sie die Datei öffnet, haben wir teilweise bereits Zugang zu diesen Systemen oder Daten.» Dies funktioniert allerdings nicht immer. In solchen Fällen gehen die Penetration Hacker selbst in das Gebäude ihrer Kunden und schliessen dort einen USB-Stick an einen Computer an. So kann ein trojanisches Pferd installiert werden. Haben sich die Hacker im Innern einer Firma erst einmal eingenistet, ist es meist ein Leichtes, sensible Daten zu kopieren oder gar Systeme zu beschädigen. Die grösste Angriffsfläche bieten dabei Programme und Systeme, die von den Unternehmen selbst entwickelt oder die schon seit vielen Jahren nicht mehr aktualisiert wurden. Brunschwiler sagt: «Grosse Dienstleister halten ihre Produkte stets aktuell und stellen regelmässig Updates bereit. Das reduziert die Gefahr, von einem Cyberangriff überrascht zu werden.»

Penetration Tests für alle Branchen

Bei grossen Banken und Versicherungen sind Penetration Tests seit mehreren Jahren etabliert, entsprechend seien viele der Systeme heute auch sehr gut geschützt. Laut Brunschwiler werde Penetration Testing auch bei Produktionsbetrieben immer beliebter. «In deren Geschäft spielen die IT und die Vernetzung von Maschinen eine immer wichtigere Rolle. Ein Ausfall der Produktionsmaschinen oder ein Diebstahl von Daten hat verheerende Folgen.» Sandro Müller, CEO von Go Security, ebenfalls ein Anbieter von Penetration Tests, sagt: «Die Kunden reichen mittlerweile vom kleinen KMU bis zu grossen Firmen. Die Bedeutung von Cybersicherheit spielt auch bei kleinen Firmen eine immer grössere Rolle.» Je nach Kunde würden jedoch Aufträge unterschiedlich definiert. «Geht es um ein spezifisches System oder eine bestimmte Funktion, die getestet werden kann, bieten wir bereits Penetration Tests für einige tausend Franken an. Ist der Auftrag jedoch breiter oder der Aufwand des Tests grösser, steigen auch die Kosten.»

Es gebe auch öffentliche Penetration Tests, sagt Müller: «Die Post lässt derzeit ihr System für E-Voting öffentlich testen. Dies ist auch eine Art Penetration Test. Jeder, der sich dafür interessiert, kann sich daran beteiligen. Üblicherweise ist es der Abschluss diverser interner Tests und aufwendig in der Planung.»

Ist ein Penetration Test abgeschlossen, wird jeweils eine umfangreiche Dokumentation für den Kunden erstellt. Damit können die Sicherheitslücken gezielt geschlossen werden. Cyrill Brunschwiler sagt mit Blick auf die Dokumentation: «Eine wichtige Information für unsere Kunden ist die Einschätzung, welche Sicherheitslücken besonders kritisch sind und schnell geschlossen werden müssen.»