Kolumne: Chief Digital Community

# IT-Sicherheit: Vorbeugen ist besser als heilen

Thomas Meier

Cyberattacken auf Schweizer Unternehmen nehmen nicht nur an Quantität, sondern auch an Qualität, Effizienz und Professionalität zu. Hier einige Learnings aus aktuellen Sicherheitsvorfällen.

Mit Sicherheit sind auch Ihnen die beinahe täglichen Berichterstattungen über erfolgreiche Cyberattacken auf Schweizer Unternehmen nicht entgangen. Klar: Wir als Cyber-Security-Experten können uns dadurch zwar erfolgreich positionieren und so manchen Kunden (den Umständen entsprechend) glücklich machen. Trotzdem sind auch wir der Meinung, dass es gar nie so weit kommen müsste. Cyber Security liegt in der Verantwortung des Managements. Deswegen unser Appell: Lernen Sie aus den vergangenen Sicherheitsvorfällen. Bedrohlicher als die schiere Menge der Angriffe ist ihre zunehmende Qualität, Effizienz und Professionalität. Gleichzeitig dauert es nicht selten Wochen, Monate oder gar Jahre, bis ein erfolgreicher Angriff erkannt wird. Denn traditionelle Sicherheitsmassnahmen erkennen typischerweise nur bekannte Malware und Angriffsmuster. Professionelle Hacker sind aber raffinierter und unterlaufen solche Systeme; sie agieren sozusagen unter dem Radar. Aktuelle Beispiele bestätigen dies leider. So wissen wir von Fällen, bei welchen die betroffenen Unternehmen mehrere Monate von einer «Emotet»-Infiltration betroffen waren, ohne es zu merken.

Es ist aber nicht so, dass bewährte Best-Practice-Massnahmen oder hochmoderne Lösungen früher oder später überholt sind – im Gegenteil! Ohne sie wären die meisten Unternehmen Cyberkriminellen schon längst zum Opfer gefallen, und so manches wohl auch in der Versenke gelandet. Die besagten Massnahmen bieten die notwendige Basis, um einen Grossteil der Attacken im Hintergrund abzuwehren. Die reine Abwehr von Angriffen ist aber zu kurz gegriffen. Heutzutage ist es unerlässlich, der Erkennung und schnellen Reaktion mehr Gewicht zu schenken. Sie müssen leider immer davon ausgehen, dass die Angreifer einen Weg in Ihr Netzwerk finden werden. Was zudem viele vergessen: Auch die innovativsten Lösungen sind machtlos gegen den Angriffsvektor «Mensch», in diesem Fall meist Mitarbeitende. Ein gutes Beispiel hierfür sind Phishing-Mails, die leider oftmals nicht als solche erkannt werden.

Mit Mensch meinen wir aber nicht nur Mitarbeitende, sondern auch das Management. So manche hochrangigen Manager respektive Führungskräfte erkennen erst bei der Analyse eines Sicherheitsvorfalls, dass das Übel mit relativ einfachen Massnahmen hätte verhindert oder zumindest das Ausmass minimiert werden können. Natürlich möchten die meisten wissen, was sie hätten besser machen können. Daher einige nicht-technische Learnings von aktuellen Incidents, damit Sie gerüstet sind, sollten Sie einmal in eine ähnliche Situation kommen.

**Persönlichkeit vor Leistungsausweis**

Gerade im Bereich der Cyber Security und erst recht bei der Reaktion auf einen Sicherheitsvorfall sind Sie natürlich darauf angewiesen, die fachlich besten Mitarbeitenden zu haben. Diese müssen in der Regel vor allem eines sein – technische, oftmals hochspezialisierte Experten auf ihrem Gebiet. Oftmals wird von den Führungskräften erwartet, dasselbe Know-how mitzubringen. Ein Trugschluss! Natürlich müssen sie auch fachliches Know-how haben, aber unsere Erfahrung zeigt: Setzen Sie bei der Leitung des Krisenstabs lieber auf eine Person, die in dieser hektischen Situation die Ruhe bewahren kann. Jemand, der seinem Team klare Anweisungen geben und koordinieren kann. Jemand, der auf Augenhöhe mit dem obersten Management kommunizieren kann. Solche Personen sind Gold wert und oftmals die besseren Führungskräfte – und zwar nicht nur in Krisensituationen. Genau dann zeigt sich, ob die Führungscrew funktioniert.

**Kommunikation ist Chefsache**

Sorgen Sie dafür, dass die leitende Person des Krisenstabs nicht selber in den «Schützengraben» steigen muss. In erster Linie muss diese den Überblick behalten. Dabei geht es vor allem darum, Aufgaben zu verteilen und zu koordinieren sowie wichtige Informationen/Erkenntnisse zu sammeln, aufzubereiten und nicht zuletzt zu kommunizieren. Die Krisenkommunikation ist ein mitentscheidender Punkt – egal ob intern oder extern. Gerade die Mitarbeitenden brauchen in dieser Situation klare und verständliche Informationen, eine emotionale Begleitung und die Präsenz des Chefs. Deshalb darf die Kommunikation nie delegiert werden. Kommunikation ist und bleibt Chefsache!

**Vertrauen ist gut, Kontrolle ist besser**

Wie bereits erläutert: Führungskräfte brauchen keine «eierlegende Wollmilchsau» zu sein – oder anders ausgedrückt Spezialisten in sämtlichen Gebieten der Cyber Security. Dafür haben diese ein Händchen, die richtigen Fachkräfte einzustellen. Cyber Security ist jedoch ein riesiges Gebiet, weshalb es sich lohnen kann, Externe herbeizuziehen – sei es in Form von Consulting, zur Überprüfung der bestehenden Infrastruktur (beispielsweise mit einem Penetration Test), Outsourcing von Bereichen wie Cyber Defence oder auch in Form von Response Services, sollte es doch zu einem Security Incident gekommen sein. Wenig überraschend wünschten sich viele unserer Kunden, die einen schwerwiegenden Vorfall hatten, solche Vorkehrungen früher ergriffen zu haben. Denn bei einem Sicherheitsvorfall zählt jede Sekunde. Denn bei einem Sicherheitsvorfall zählt jede Sekunde – somit ein definitiv schlechter Zeitpunkt, um erst jetzt mit der Evaluation eines Experten zu beginnen. Deshalb gilt: Sie müssen in «Friedenszeiten» wissen (und intern geregelt haben), an wen Sie sich wenden können, und zwar 24/7!

**Klare Prozesse sind Gold wert**

Das Definieren von Prozessen und Strukturen für einen allfälligen Sicherheitsvorfall – oder auch einfach «nur» für den ordentlichen Betrieb – ist keine beliebte oder gefühlt dringende Aufgabe. Wir hören deshalb oft: «Wir sind für einen Angreifer nicht interessant und haben keine wichtigen Daten.» Nicht selten ein fataler Irrtum, wie unsere Erfahrung zeigt. Nehmen Sie sich die Zeit für die Erarbeitung eines (Notfall-)Handbuchs, denn woran sollen Sie und Ihr Team sich in Krisensituationen sonst halten? Und glauben Sie uns – in einer Krisensituation ist es zumindest in einer ersten Phase schwierig, klar und strukturiert zu denken. In dieser Hinsicht ist es ebenso wichtig zu definieren, wer für was, wie, wann und in welcher Regelmässigkeit verantwortlich ist. Die regelmässige Erstellung von Back-ups und die Durchführung von Schwachstellen-Scans, die Installation von Patches oder die Sensibilisierung der Mitarbeitenden sind beispielsweise simple, aber durchaus effektive präventive Massnahmen. Trotzdem sehen wir immer wieder, dass solche Punkte vergessen werden.

Wir als Cyber-Security-Experten wissen aus zahlreichen Sicherheitsvorfällen bei Kunden, dass aller Anfang schwer ist. Nehmen Sie sich die (natürlich nicht abschliessenden) Tipps zu Herzen. Setzen Sie das Thema Cyber Security ganz oben auf die Agenda. Und mit «Sie» ist auch das oberste Management gemeint – denn das Risikomanagement ist eine Führungsaufgabe. Sorgen Sie für ausreichend personelle und finanzielle Ressourcen. Und nicht zuletzt, suchen Sie sich einen Cyber-Security-Experten, der Sie vor und schlimmstenfalls während sowie nach einer Cyberattacke begleitet. «

*Thomas Meier ist CEO der auf Cyber Security spezialisierten Infoguard AG und Vorstandsmitglied der Chief Digital Community CDC.*
*www.infoguard.ch, www.chiefdigital.ch*


KMU-Magazin Nr. 11/12, November/Dezember 2019