IT-Sicherheit und Cloud-Management I

Sicherheitsrisiken erkennen und reduzieren

Die ohnehin schon wachsende Zahl an Cyberangriffen auf Unternehmen hat wegen der sich verändernden Arbeitsbedingungen neue Nahrung erhalten. Um Schaden vom eigenen Unternehmen abzuwenden gilt es, IT-Sicherheitsrisiken richtig einzuschätzen und entsprechende Vorkehrungen zu treffen. Ein Überblick.

› Fabio Poloni

Produkte und Dienstleistungen auf die Kundenbedürfnisse und -wünsche anzupassen und dabei Spitzenarbeit zu leisten, gehört zu den Kernkompetenzen von Schweizer KMU. Dagegen tun sie sich häufig schwer, ihre IT-Sicherheitsrisiken richtig einzuschätzen.

Einfallstor Internet

Die Verantwortung des Risikomanagements – auch in der Informatik – fällt in den Bereich der Geschäftsleitung. Als Erstes muss sich diese einen Überblick über die Arbeitsabläufe und die dafür benötigten Daten verschaffen und für sich festlegen, welchen Stellenwert die Informationssicherheit und der Schutz der Daten in ihrem Unternehmen haben sollen. Anschliessend kann sie die IT-Verantwortlichen ins Boot holen und Mittel und Ressourcen für die nötigen Optimierungsschritte reservieren.

Die zentralen Fragen: Welchen Gefahren ist die IT-Sicherheit eines KMU überhaupt ausgesetzt? Worauf soll das Augenmerk gerichtet werden? Bedrohungen für elektronische Daten gelangen (unbemerkt) über das Internet ins Haus. Viren, Würmer, Trojaner, Spyware, Keylogger und Co. verstecken sich gerne in E-Mails, aber auch auf unseriösen Websites, in Werbeanzeigen und auch in privaten Mitteilungen, die via SMS, Whatsapp oder soziale Netzwerke eingehen. In vielen unerwarteten Nachrichten werden die Empfänger unter verschiedensten Vorwänden aufgefordert, auf einen Link zu klicken. Diese Links können auf Websites leiten, welche nach Login-Daten fragen oder auch Anhänge zum Herunterladen anbieten. Präparierte Anhänge (Office-Dateien, ZIP-Archive) können beim Öffnen Systeme infizieren, oftmals ohne dass die Nachrichtenempfänger dies merken. Sehr verbreitet sind Ransomware-Schadprogramme. Sind diese einmal in einem Netzwerk, können sie alle Daten verschlüsseln und sich auf andere Systeme weiterverbreiten. Die Cyberkriminellen verlangen dann Lösegeld und versprechen im Gegenzug, die Daten wieder zu entschlüsseln. Ob dies auch tatsächlich passiert, kann man im Voraus nicht sagen.

kurz & bündig

- IT-Sicherheit kann grob in drei Kategorien eingeteilt werden: Prävention, Detektion und Reaktion.
- Sehr verbreitet sind Ransomware-Schadprogramme. Sind diese einmal in einem Netzwerk, können sie alle Daten verschlüsseln und sich auf andere Systeme weiterverbreiten.
- Das Wichtigste ist die Erstellung von regelmässigen Sicherungskopien aller relevanten Daten. .

Zunehmende Raffinesse

Erkennbar sind solche Nachrichten oft an fehlerhafter Rechtschreibung und Grammatik, an der allgemeinen, unpersönlichen Ansprache und an dringlichen oder angsteinflössenden Formulierungen. Meist enthalten die Nachrichten zusätzlich Anhänge oder Links. Es gibt jedoch inzwischen auch sehr raffinierte E-Mails, in denen selbst der Absender und der Inhalt so gestaltet sind, dass die Empfänger denken, die Mail komme von ihrer Buchhaltungsabteilung, ihrer Bank oder einem bekannten geschäftlichen

Kontakt. Geht es um Geld, um Passwörter oder andere sensible Daten, ist immer eine persönliche Rücksprache mit dem vermeintlichen Absender erforderlich (Überprüfung der Echtheit der Mail). In den vergangenen Monaten haben Spezialisten vermehrt beobachtet, dass der Schadcode die E-Mail-Nachrichten von seinen Opfern stiehlt und dann ganze Mailverläufe inklusive infizierter Anhänge an deren Kontakte schickt. Zudem können auch SMS und Anrufe (die Anzeige der Telefonnummern) manipuliert werden.

Vorkehrungen treffen

Der Mensch mit seiner Gutgläubigkeit und seiner Hilfsbereitschaft ist das beliebteste Ziel für Hacker. Es gibt aber wertvolle Unterstützung seitens der Technik. Diese vier Vorkehrungen sollten unbedingt getroffen werden:

- Das Wichtigste ist, Sicherungskopien aller relevanten Daten regelmässig zu erstellen. Dabei sollen die Kopien nicht auf einem Laufwerk im Netzwerk liegen, da das trojanische Pferd auch dieses mitverschlüsseln würde. Relevant ist auch, dass überprüft wird, ob die Datensicherung und vor allem die Wiederherstellung der Daten funktionieren.
- Aktuelle Virenschutzprogramme auf allen Geräten installieren – also auch auf Laptops oder anderen mobilen Geräten.
- Auch die Software muss auf dem neuesten Stand sein. Werden die Update-Empfehlungen der Hersteller übernommen, werden regelmässig allfällige Fehler behoben und Schwachstellen geschlossen.
- Virtuelle Brandschutztüren, sogenannte Firewalls, einsetzen: Sie schützen Computer und Server gegen aussen und separieren sie untereinander in verschiedenen Netzwerken. Die Ausbreitung von Schadsoftware wird dadurch stark eingeschränkt. Ein Plus: Dieses Vorgehen verbessert auch die Wartbarkeit des Netzwerkes.

Einstellungen anpassen

Werden neue Netzwerk- und Serverkomponenten in Betrieb genommen (zum Beispiel Datenbanken, Router, Switches), vertraut man gerne auf die Werkseinstellungen des Herstellers. Diese sind aber meistens weniger auf Sicherheit ausgelegt, sondern darauf, in vielen unterschiedlichen Umgebungen möglichst wenig Probleme zu verursachen. Es ist deshalb

zu empfehlen, die Einstellungen regelmässig zu prüfen und diese an heutige Bedürfnisse und Standards anzupassen. Auch hier erhöht das Bewusstsein für die unterschiedlichen Einstellungen die zusätzliche Wartbarkeit und bringt der System-Administration ein besseres Verständnis für die Systeme.

Cloud und Sicherheit

KMU profitieren von der Digitalisierung, wenn es um die eigene IT-Infrastruktur geht. Durch die zunehmende Vernetzung können Dienste (Speicherplatz, Rechenleistung, Software etc.) kostengünstig und schnell in die Cloud ausgelagert werden. Lokale Infrastrukturen sind dagegen oft teuer und weniger flexibel (Stichwort Skalierbarkeit, Bereitstellung). Cloud-Services sind relativ leicht zu konfigurieren, doch sind sie auch sicher?

Cloud-Services von den Weltmarktführern schützen ihre Anlagen mit viel Aufwand und sind tendenziell sicherer als Cloud-Dienste, die ein KMU selber betreibt oder bei Nischenanbietern beziehen könnte. Eine Fachperson kann über alle Vor- und Nachteile von Cloud-Computing beraten, sodass abgewogen werden kann, welche Daten dafür in Frage kommen sollen. Beim Thema «Shared Responsibility» ist klar festzulegen, welche Verantwortung und welche Kontrollfunktionen beim KMU und welche beim Cloud-Anbieter liegen. Ein Tipp: Ausgeschiedene Mitarbeitende sollten weder physischen noch virtuellen Zutritt zum Unternehmen haben. Die IT-Administration muss also nach einem Austritt auch die Cloud-Accounts sperren.

Wissen ist Macht

Benutzername und Passwort sind einmalig und streng geheim. Werden die Login-Daten für einen Hacker zugänglich, hat dieser die Zugriffsberechtigung auf eine oder mehrere Anwendungen und die darin gelagerten Geschäftsinformationen. Ein sicherer Umgang mit Passwörtern im ganzen Unternehmen ist deshalb essenziell. Wertvolle Tipps dazu gibt die Melde- und Analysestelle (MELANI) des Bundes. Wenn Menschen über ein Thema viel wissen, können sie bessere Entscheidungen treffen. Über IT-Sicherheit muss also gesprochen werden. Die Mitarbeitenden sollen aufgeklärt und für Sicherheitsthemen sensibilisiert werden. Mit dem nötigen Rüstzeug können sie dann verantwortungsvoll handeln. Um rasch und gezielt auf mögliche Vorfälle reagieren zu können, braucht es eine Sicherheitskultur, in der Mitarbeitende sich umgehend melden, wenn sie in eine Falle getappt sind oder einen Verdacht haben.

IT-Sicherheitsstrategie

IT-Sicherheit kann grob in drei Kategorien eingeteilt werden: Prävention, Detektion und Reaktion. Die zweite und dritte Kategorie befasst sich mit Vorgehensweisen, wenn trotz aller Vorsichtsmassnahmen ein Vorfall (Incident) passiert. Mit der IT-Administration und Fachleuten ist zu klären, wie Ereignisse detektiert werden und was in solchen Fällen getan wird. Schnelles und überlegtes Handeln ist gefragt. Fehler und Verzögerungen kosten unter Umständen sehr viel Geld. Der Vorfall soll am Schluss auch aufgearbeitet werden: Ursachen finden, Schadensermittlung, Wiederherstellung, Verbesserungen, neue Erkenntnisse etc. Sind die Grundempfehlungen umgesetzt und ist die Belegschaft geschult, heisst es dranbleiben, denn IT-Sicherheit ist ein Prozess und kein Zustand. In einem weiterführenden Schritt kann die IT-Sicherheit von einer unabhängigen Fachperson geprüft werden. Ein Security Assessment gibt einen aussagekräftigen Überblick über den Sicherheitszustand der IT-Infrastruktur und mittels simulierter Cyberangriffe können Sicherheitslücken in Systemen und Anwendungen identifiziert werden. Zudem gibt es Fachleute, welche IT-Abteilungen bei einem Cyber-Notfall unterstützen und durch die verschiedenen wPhasen der Vorfallbehandlung (Sofortmassnahmen einleiten, Ausbreitung eindämmen, Analyse etc.) begleiten. «

Check-up: IT-Sicherheit

- Verantwortlichkeiten regeln
- Backups erstellen, Virenschutzprogramm installieren, Firewall aktivieren, Software aktuell halten
- Aufmerksam sein
- Einsatz von Cloud-Services genau abklären
- Passwörter geheim halten
- Mitarbeitende sensibilisieren und schulen
- Für den Notfall vorsorgen
- IT-Systeme und Netzwerke überprüfen lassen

Porträt

Fabio Poloni
Security Analyst, Compass Security Schweiz AG

Kontakt

fabio.poloni@compass-security.com, www.compass-security.com