IT-Sicherheitskonzepte: Im Mittelstand besteht Nachholbedarf

Veröffentlicht: 09. August 2017

Sicherheitsmaßnahmen im Bereich IT sind heutzutage gang und gäbe. Aber reichen ein paar Maßnahmen aus, um ein berechtigtes Gefühl von Sicherheit zu vermitteln?

Viele Unternehmen betrachten IT-Sicherheit noch sehr statisch, regelmäßige Revisionen werden eher selten für notwendig erachtet. Der dadurch entstehende falsche Sicherheitseindruck öffnet Dritten oftmals Tür und Tor für unberechtigte Zugriffe. Wichtig sind eine umfassende Bestandsaufnahme inklusive Identifizierung eventuell bestehender Sicherheitslücken und ein darauf aufbauendes Sicherheitskonzept.

Wo liegen die Sicherheitslücken?

KMUs benötigen einfache Lösungen, die sämtliche potenzielle Angriffspunkte berücksichtigen. Das System sollte automatisch überwachen, im Bedarfsfall selbständig agieren oder den zuständigen Mitarbeiter informieren können. Dafür bietet der Markt cloudbasierte Lösungen an, die lokale Ressourcen nicht belasten und keine komplexe Infrastruktur im Unternehmen voraussetzen.

Handlungsbedarf besteht in mittelständischen Unternehmen, wenn keine oder eine mangelhafte Systemlandschaft mit nicht gepatchten Applikationen besteht. Die gewachsenen Strukturen sind häufig entweder gar nicht oder nur ungenügend dokumentiert worden. Diese Intransparenz stellt ein hohes Gefährdungspotenzial dar.

Sicherheitslücken entstehen oft dadurch, dass relativ kleine IT-Abteilungen meist mit ihrer täglichen Arbeit und der Administration vorhandener Applikationen vollauf beschäftigt sind. Der Betrieb einer komplexen Sicherheits-Infrastruktur kommt dann aus personellen Gründen zu kurz.

IT-Sicherheitskonzept als Lösung

Gute IT-Sicherheitskonzepte funktionieren nach einem ganzheitlichen Ansatz. Die Sicherheit der IT-Infrastruktur eines Unternehmens kann nicht an bestimmten Punkten fixiert werden, alle Bereiche müssen durch eine umfassende Strategie abgedeckt sein.

Die Anforderungen an ein solches System sind vielfältig, vom WLAN-Zugang über Serverfarmen bis zum Client reicht der Schutzbedarf. Dabei muss die Lösung höchstmögliche Transparenz

bieten ohne das laufende Tagesgeschäft zu beeinträchtigen.

Ein profundes IT-Sicherheitskonzept beschränkt sich nicht auf den Einsatz von einzelner Schutzsoftware. Das gesamte Konstrukt muss in eine permanent zu aktualisierende Organisationsstruktur integriert werden. IT-Sicherheitsmanagement verlangt die Regelung von Zugriffen und Berechtigungen. Ferner muss die Sicherheitslösung bei aller Komplexität jederzeit in der Lage sein, im Bedarfsfall schnell zu reagieren. Die IT-Infrastruktur eines Unternehmens kann nur dann als sicher bezeichnet werden, wenn eine dokumentierte Prozedur für die Rekonstruktion von Daten vorhanden ist. Dafür braucht es ein funktional geprüftes System für die Wiederherstellung eines kompromittierten Systems oder von Dateien.

So schließen sich Sicherheitslücken

Der erste Schritt zur Lösung des Problems ist, wie so häufig, die Erkenntnis. Der Unternehmer muss die Notwendigkeit eines IT-Sicherheitskonzepts verstehen und zunächst für Transparenz bezüglich seiner vorhandenen Systeme, bestehenden Zugriffsmöglichkeiten und ausgeführten Applikationen sorgen. Dann hat er die komplexesten Schritte hin zu einem effizienten IT-Sicherheitskonzept bereits getan.

Das Verständnis von IT-Sicherheit generell beinhaltet, dass in technischer Hinsicht kein offensichtlicher Vorteil entsteht. Die IT-Abteilung und sämtliche Anwender innerhalb des Unternehmens schaffen mit der Berücksichtigung von Sicherheitsmaßnahmen eine gemeinsame Basis für den effektiven Schutz ihres Arbeitsumfeldes. Dieser entscheidende Vorteil muss bei der Einführung eines neuen Systems offen kommuniziert werden. Mit Kosteneinsparungen kann in diesem Fall nicht argumentiert werden, denn ein IT-Sicherheitskonzept funktioniert im Grunde genommen wie eine Versicherung. Hier wird ein Invest getätigt, das mögliche Schäden abwenden soll, die wiederum hohe finanzielle Einbußen nach sich ziehen könnten.

Sicherheit auf aktuellstem Stand

Ein optimales IT-Sicherheitskonzept funktioniert auf lange Sicht. Nach der Einführung ist ein zuverlässiger Support für die permanente Funktion des Systems unabdingbar. Regelmäßig ausgeführte Reviews der Sicherheitsfunktionen müssen ständig die Zweckmäßigkeit des Schutzes gegen aktuelle Bedrohungen überprüfen. Die größte Herausforderung ist dabei das Klassifizieren von Bedrohungen in Bezug auf den individuellen Schutzbedarf.

Aktuell bekannt gewordene Ereignisse zeigen, dass IT-Angriffe immer komplexer und detaillierter vorbereitet werden. Das Angriffsziel liegt häufig nicht mehr in der Infrastruktur selbst, sondern wird auf den einzelnen Mitarbeiter ausgerichtet. Dadurch können getroffene Schutzmaßnahmen umgangen werden, indem der Mitarbeiter ohne seine Kenntnis dazu veranlasst wird, schadhafte Tätigkeiten auszuführen.

Das kriminelle Potenzial steigt in diesem Bereich bedrohlich an. Die Entstehung eines lukrativen Marktes wird beobachtet. Schadprogramme wie beispielsweise Ransomware werden inklusive professionellem Support in den entsprechenden Kreisen feilgeboten. Nach

Veröffentlichung kommen die Programme in abgewandelter Form mehrfach zum Einsatz. In der Folge können signaturbasierende Prüfverfahren solche abgeänderte Schadsoftware nicht mehr erkennen. Die sichere IT-Zukunft liegt deshalb in Verfahren, die Auffälligkeiten in der Infrastruktur erkennen und umgehend darauf reagieren können. Abschließend gilt festzuhalten, dass klassische Sicherheitsvorkehrungen auf unterer Infrastrukturschicht durch intelligente Maßnahmen zur Applikationsüberwachung ergänzt werden müssen um im Gesamtkontext eine globale Sicht aller Kommunikationsbeziehungen zu erhalten.

Jetzt handeln für künftige Sicherheit

Unternehmen wie QOSIT, die ihre Kunden bei der Entwicklung eines IT-Sicherheitskonzepts unterstützen, schauen über den Tellerrand hinaus in eine möglichst sichere Zukunft. Denn IT-Fachleute sind sich der Tatsache bewusst, dass die Bedrohungen immer komplexer werden. Systemhersteller, IT-Administratoren und Anwender müssen mit Angriffen aus unerwarteten Richtungen rechnen. Denn die Vernetzung von Geräten rund um den Erdball schreitet fort, parallel wächst die Zahl der potenziellen Angreifer. Weltweit stehen den Kriminellen somit zahlreiche Ausgangsquellen zur Verfügung, von denen aus sie ihre Angriffe initiieren können. Die kleinen IT-Abteilungen von KMUs sind mit dieser Herausforderung alleine meist überfordert.

Matthias Schmidt, Teamleiter Professional Service bei QOSIT

www.qosit.com