Link: https://www.cio.de/a/it-sicherheit-im-mittelstand,2958621

Schritt für Schritt

IT-Sicherheit im Mittelstand

Datum: 28.05.2014
Autor(en): Oliver Häußler

In mittelständischen Unternehmen bestehen häufig Unsicherheiten im Umgang mit Themen wie Cloud und Mobile. HP-Sicherheitsexperten empfehlen, ganzheitlich über die Sicherheit nachzudenken, aber mit konkreten Einzelthemen zu starten.

IT-Sicherheit ist ein weites Feld. Es umfasst die sogenannten Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität. Um eine ganzheitliche IT-Sicherheitsvorkehrung zu treffen, fehlt es vielen Unternehmen meist an Personal wie auch an Wissen. "Zwar gibt es bei etwas größeren Mittelstandsunternehmen in der Regel Richtlinien, die die Themen IT- und Informationssicherheit darstellen", stellt Sebastian Köhler, Security Consultant Executive bei **HP Enterprise Services**[1], fest, aber diese werden "oft nicht oder unzureichend dokumentiert beziehungsweise umgesetzt, und es fehlen häufig organisatorische Konzepte". Es mangelt an vielen Stellen, nicht zuletzt auch daran, dass es nur selten Security- oder Compliance-Verantwortliche gibt, was dazu führt, "dass Security nebenher betrieben wird", so Köhler.

Dramatischer Anstieg der Cyber-Attacken

Nicht ohne Folgen: Jedes zweite Unternehmen war bereits Ziel einer Cyberattacke. Da die Anzahl der Angriffe seit 2010 um über 70 Prozent zugenommen hat, ist auch künftig mit einer erhöhten Bedrohung zu rechnen. Allerdings bemerken die Betroffenen meist nichts davon. Denn es vergehen durchschnittlich 243 Tage, bis ein Sicherheitsverstoß aufgedeckt wird.

Diese Zahlenbeispiele, die Marktforschungsunternehmen wie **Forrester Research**[2], Ponemon Institute und Coleman Parkes Research ermittelten, zeigen die Situation der IT-Sicherheit von Unternehmen jeglicher Größe an. Speziell beim deutschen Mittelstand ist die Sicherheitsgefahr noch gravierender. Schließlich sind mittelständische Unternehmen in Deutschland wirtschaftlich sehr erfolgreich und verfügen über entsprechend schützenswertes Know-how. Allerdings ist die notwendige integrierte Security für sie eine große Herausforderung. So stellt die Untersuchung "IT-Sicherheitslage im Mittelstand 2013", die von der DsiN zusammen mit dem Innenministerium durchgeführt wurde, Handlungsbedarf fest bei den Themen "Sichere Nutzung mobiler Endgeräte", "Cloud Computing sicher und rechtskonform nutzen" sowie "E-Mail-Sicherheit".

Sebastian Köhler, Security Consultant Executive HP Enterprise Services: "Häufig fehlen organisatorische Konzepte"
Foto: HP Deutschland

Alle Geschäftsprozesse sind IT-abhängig

Köhler appelliert an die Unternehmen, besser über Sicherheit nachzudenken. Inzwischen sind nahezu alle Geschäftsprozesse IT-abhängig, "aber der Mittelstand kennt den Grad der Abhängigkeit häufig nicht und weiß nicht, wie relevant sie sind und wie lange das Unternehmen überleben kann, wenn diese unterbrochen werden". Bricht beispielsweise das Bestellsystem bei einem Onlinehändler zusammen, kann ihn der Ausfall jede Minute große Summen kosten. Manchmal sind es ganz einfache Dinge, die einen Prozess zum Stillstand bringen: Fällt beispielsweise der Etikettendrucker im Logistikzentrum aus, kann nichts mehr versandt werden - der Geschäftsprozess ist unterbrochen.

Köhler setzt bei der Sicherheitsberatung eben da an. "Die erste Aufgabe ist es, die Geschäftsprozesse zu verstehen und sie zu analysieren. Danach arbeitet man sich pyramidenartig herunter, prüft, wo die Risiken liegen, und adressiert die Themen Verfügbarkeit, Vertraulichkeit und Integrität". Um nicht nach dem Gießkannenprinzip ein überproportioniertes Sicherheitskonzept aufzubauen, werden schützenswerte und weniger schützenswerte Daten im ersten Schritt kategorisiert und klassifiziert. Köhler: "Die sogenannten Kronjuwelen, also die zu schützenden Unternehmenswerte, bekommen höchste Priorität". Oft liege der Anteil an Kronjuwelen nur bei einem Prozent aller Informationen, stellt Jörg Eggers, Chief Technologist für Mittelstandskunden bei **HP Enterprise Services**[3], fest. "Das können strategische Dokumente sein, Dokumente über Zukäufe oder Prototypenentwicklung oder anderes Unternehmens-Know-how". Für die Kronjuwelen wird der optimale Schutz erarbeitet, für die anderen Daten reicht ein niedrigeres Schutzniveau. Eggers empfiehlt eine "Ausgewogenheit zwischen Sicherheit und Funktionalität".

Im zweiten Schritt wird untersucht, wo die Daten liegen. "Es kommt schon mal vor, dass jemand wichtige Kennzahlen auf seinem vermeintlich sicheren USB-Stick speichert, den er oder sie abends mit nach Hause nimmt", so Eggers. Das können Kreditkartennummern inklusive Prüfziffern sein, da mit diesen Daten regelmäßig die Reisen der Mitarbeiter gebucht werden. Sicherheitstechnisch betrachtet ist das natürlich völlig inakzeptabel und erfordert eine klare Regelung, wo welche Daten zu liegen haben. Zusätzlich ist eine Schulung durchzuführen, und die Mitarbeiter müssen für das Thema besser sensibilisiert werden.

Im dritten Schritt werden sowohl für die streng vertraulichen als auch für alle anderen Daten organisatorische und technische Maßnahmen in Bezug auf Aufnahme, Verarbeitung, Zugriffs- und Löschungsrechte festgelegt.

Verfügbarkeit: Was ist, wenn…?

Einer aktuellen Studie von Techconsult zufolge variieren die entstandenen Kosten bei einem Systemausfall im Mittelstand im Durchschnitt zwischen 25.000 Euro bis knapp 41.000 Euro. Bei der ganzheitlichen Betrachtung sollte das Thema Verfügbarkeit aber immer im Kontext mit der Vertraulichkeit stehen. Es geht darum, Ausfallkonzepte zu entwickeln, die kritische Fragen zu beiden Themen beantworten: Was passiert, wenn ein Netzwerkswitch ausfällt? Wo liegen Daten der Verbraucher? Was passiert, wenn ein Laptop oder ein Tablet-PC verloren gehen? Werden dort gespeicherte Daten für den Geschäftsprozess benötigt? Was geschieht, wenn es sich dabei um kritische Daten handelt? Eggers: "Die Folgen müssen auch aus strategischer Sicht betrachtet werden, egal, warum etwas ausfällt."

Zur ganzheitlichen Betrachtung gehört außerdem das Thema Integrität - darunter werden Schutzmaßnahmen verstanden, die dazu beitragen, dass niemand unberechtigt und unbemerkt Daten verändern kann. Weitere Themen, die es zu berücksichtigen gilt, sind Compliance, Mitarbeiterschulung, Verantwortlichkeiten für Sicherheitsthemen und viele mehr. Überblick und Orientierung über Vorgehensweise und Methodik bieten der Standard ISO/IEC 27001:2013 aus internationaler Sicht sowie der IT-Grundschutz, um ein ganzheitliches Sicherheitskonzept im Unternehmen aufzubauen sowie angemessene Sicherheitsmaßnahmen zu identifizieren und umzusetzen.

Jörg Eggers, Chief Technologist für Mittelstandskunden HP Enterprise Services: Höchste Priorität für Unternehmens-Kronjuwelen
Foto: HP Deutschland

Angst vor der "Büchse der Pandora"

Laut Eggers und Köhler ist das Verständnis für IT-Sicherheitsthemen beim Mittelstand in den vergangenen Jahren gewachsen. Jedoch zögern viele damit, die entsprechenden Schritte zur Umsetzung in die Wege zu leiten, weil Sie Angst davor haben, die "Büchse der Pandora" zu öffnen, in der ein unbekanntes Ausmaß an Sicherheitsproblemen sichtbar wird. Dabei raten die HP-Experten, genau diesen Ansatz zu verfolgen: mit einem aktuellen Thema zu beginnen und anschließend systematisch weitere relevante Sicherheitsthemen aufzubereiten.

Eine typische Vorgehensweise in der Praxis kann beispielsweise die Erarbeitung folgender drei Aspekte sein:

1. Einstieg über das Thema Mobile Security, das derzeit viele Unternehmen bewegt.

2. Penetration-Tests: Dazu gehören Netzwerktests, die Überprüfung von Web-Apps sowie die Wireless-Funktionalität.

3. ISO-27001-Assessment: Einen Überblick verschaffen, wie das Unternehmen hinsichtlich IT-Sicherheit aufgestellt ist.

Gerade wenn es im Unternehmen keinen dedizierten Sicherheitsverantwortlichen gibt und das Fachwissen für den Aufbau eines wirkungsvollen und realisierbaren Schutzes der Unternehmenswerte fehlt, sollten mittelständische Unternehmen entweder diese Rolle implementieren oder externe Unterstützung in Anspruch nehmen. Aus rechtlicher Sicht ist die Unternehmensleitung ohnehin dazu verpflichtet und haftbar für den sicheren Betrieb, der nur durch Transparenz eine abgewogene Maßnahmenplanung ermöglicht.

Fazit: In puncto IT-Sicherheit hat der Mittelstand akuten Handlungsbedarf. Denn das bisher vielfach praktizierte Prinzip "Augen zu und durch" funktioniert im Zeitalter von Big Data, Cloud Computing und Mobility nicht mehr.

Links im Artikel:

[1] **http://h40047.www4.hp.com/enterprise-services/**
[2] **http://www.forrester.com/home/**
[3] **http://h40047.www4.hp.com/enterprise-services/**
