Neue IT-Risiken im Mittelstand

Schutzschilder wie Virenscanner und Firewall reichen nicht mehr aus, um Sicherheit zu gewährleisten.

Von **Holger Gerlach***

Mit immer mehr IT im Unternehmen steigt auch das Risiko. Viren, Würmer und Hacker, die über das Internet ins Firmennetz eindringen, sind bekannte Gefahrenquellen. Die Abwehrmechanismen sind mittlerweile ausgereift. Neue Anforderungen an die Sicherheitssysteme entstehen hingegen durch bislang kaum bekannte Angriffsmuster.

Persönliche Ansprache als Lockmittel

Mit der fortschreitenden Digitalisierung der Abläufe in mittelständischen Unternehmen verändern sich auch die Risiken. Dies wird am Beispiel der zunehmenden Kommerzialisierung der Hacker-Szene deutlich. Waren früher meistens Zufall und Spieltrieb die Auslöser für entsprechende Sicherheitsvorfälle, stehen heute Betrugsinteressen im Vordergrund. Diese Entwicklung spiegelt sich beispielsweise in gezielten Angriffen wie dem „Spear Phishing“ wider. Bei dieser Variante des bekannten Phishing-Angriffs werden einzelne Personen im Unternehmen mit maßgeschneiderten E-Mails attackiert. Ziel des Angriffs ist, den PC des Opfers mit einem Trojaner zu infizieren, um einen Zugang ins Netz zu erlangen. Indem die Mails den Anwender mit persönlichen Informationen ansprechen, sollen sie ihn bewegen, den Dateianhang zu öffnen oder einen manipulierten Link anzuklicken. Als Quelle dafür dienen unter anderem Social Networks und Beiträge in Internet-Foren.

Ein erfolgreicher Angriff führt häufig zum Datenklau, der in Versuche, das betroffene Unternehmen zu erpressen, oder Spionage münden kann. Solche Vorfälle sind auch im deutschen Mittelstand belegbar. Deutlich wird an diesem Beispiel auch, wie gut getarnt Angriffe sein können. Ausgangspunkt ist die Veröffentlichung scheinbar harmloser Informationen in öffentlichen sozialen Netzen und an anderen Stellen im Internet durch einen Mitarbeiter.

IT-Ausfall verursacht finanziellen Schaden

Kritisch sind solche Angriffe auch, weil sie die Verfügbarkeit der IT bedrohen. Die Computerisierung durchdringt unmerklich alle Unternehmensteile. Schritt für Schritt wurden Produktionsstraßen in das Firmennetz

Fotos: Fotolia/Feng Yu

integriert, Klemmbretter durch WLAN-fähige PDAs ersetzt und die herkömmlichen Telefonkabel gegen Ethernet getauscht. Diese Entwicklung sorgt seit Jahren für eine steigende Produktivität – aber auch für mehr Anfälligkeit. Ein Festplatten-Crash in zentralen IT-Systemen kann nun beispielsweise dazu führen, dass die komplette Produktion ausfällt; ein defektes ERP-System entzieht den Mitarbeitern ihre wichtigste Arbeitsumgebung. Eine unzuverlässige IT kann enormen finanziellen Schaden anrichten.

Im Rahmen einer umfassenden Sicherheitsstrategie gilt es zudem, viele gesetzliche Vorgaben zu beachten. Mängel in der IT-Sicherheit können zu Wechselwirkungen führen. Kommt es zu Vorfällen, weil Risiken unterschätzt wurden, drohen rechtliche Konsequenzen. Wichtige IT-relevante Gesetze sind das Bundesdatenschutzgesetz (BDSG), das Gesetz zur Kontrolle und Transparenz im Unternehmen (KonTraG) und der Sarbanes-Oxley Act (SOX). Verstöße gegen das BDSG bescheren derzeit vielen Unternehmen Negativschlagzeilen. Meistens hängen solche Verstöße direkt oder indirekt mit dem IT-Einsatz zusammen. Der Imageschaden lässt sich dabei selten in Euro beziffern. Bilanzwirksame Belastungen entstehen aber in jedem Fall durch Bußgelder, die der Gesetzgeber immer wieder erhöht.

Der Gesetzgeber verlangt eine sichere IT.

Wie wertvoll ist die eigene IT?

Viele Risiken hängen damit zusammen, dass Unternehmen ihre Abhängigkeit von IT nicht kennen. Komplexe Methoden für das Risiko-Management und konkrete Sicherheitsvorkehrungen helfen hier nur bedingt weiter. Um mit der Bedrohung angemessen umgehen zu können, muss zunächst Klarheit darüber geschaffen werden, wie die IT in die Geschäftsprozesse eingreift und wo Unternehmenswerte in Form von Daten gespeichert werden. Ist das nicht bekannt, sind Fehleinschätzungen und unzureichende Vorkehrungen unvermeidbar. Sicherheitsvorfälle und Fehlinvestitionen sind die Konsequenzen.

Die Intransparenz in Sachen IT-Abhängigkeit löst eine Kettenreaktion aus, an deren Ende eine mangelhafte Systemadministration und der unsensible Umgang mit IT-Systemen durch die Anwender stehen. Risikobewusstsein lässt sich in diesem Bereich nur dann schaffen, wenn alle Beteiligten sich über die Abhängigkeit des Unternehmens von der IT im Klaren sind. Der erste Schritt dazu ist, dass die Geschäftsführung den Stellenwert der IT kennt und IT-Risiken als unternehmenskritischen Faktor akzeptiert. Die Unternehmensleitung sollte die Anforderungen an die IT-Sicherheit in einem Strategiepapier dokumentieren und der gesamten Belegschaft mitteilen. Das verschafft den IT-Verantwortlichen Rückendeckung, wenn sie unpopuläre Sicherheitsmaßnahmen in den Fachbereichen durchsetzen müssen. Wird die IT jedoch von der Geschäftsleitung stiefmütterlich behandelt, kann ein sensibler Umgang mit IT-Anwendungen und -Systemen auch von den Benutzern kaum erwartet werden.

Transparenz schaffen

Eine wichtige Frage ist, wie sich die IT-Abhängigkeit transparent darstellen und ein angemessenes Risiko-Management einführen lässt. Die Lösung liefert das Informationssicherheits-Management-System (ISMS). Die internationale Norm ISO/IEC 27001 formuliert Anforderungen an Einführung, Betrieb, Wartung und Verwaltung eines ISMS. Die Norm schlägt zudem Arbeitsschritte vor, die etwa die verwendeten IT-Anwendungen den Geschäftsprozessen zuordnen und die sensiblen und wertvollen Daten des Unternehmens identifizieren. Daraus resultieren simple Kennzahlen wie etwa die Anzahl unentbehrlicher IT-Anwendungen und -Systeme pro kritischen Geschäftsprozess. Mit dieser Erhebung lassen sich Risiko und Auswirkungen fundiert einschätzen.

Die gemeinsame Betrachtung der Geschäftsprozesse schafft auch eine gute Kommunikationsbasis zwischen Geschäftsleitung und IT-Leitung. Mit dem Rückhalt des Unternehmens-Managements kann die IT ihre Strategie in der Kommunikation gegenüber den Fachbereichen verbessern. Statt vor Risiken zu warnen, kann sie künftig Lösungen bieten. Das bedeutet konkret, dass sie IT-Sicherheit nicht mehr auf Basis von Warnungen und Angstszenarien durchsetzen muss. Die transparente Darstellung der unternehmensweiten IT-Abhängigkeit verbessert das Risikobewusststein und das Verständnis, wenn technische und organisatorische Veränderungen erforderlich sind.

Relevante Risiken erkennen

Solange die IT weiter die Unternehmensprozesse durchdringt, werden sich auch die Risiken erhöhen. Komplexe Methoden des Risiko-Managements bleiben wirkungslos, solange nicht alle Verantwortlichen den Ist-Zustand kennen und Einigkeit über Maßnahmen erzielen. Ein prozessbasierendes Informationssicherheits-Management ist das Fundament für eine erfolgreiche Bekämpfung beziehungsweise eine Verringerung von IT-Risiken. Anstatt Security im Gießkannenprinzip einzuführen, lassen sich Risiken genau einordnen und mit angemessenem Aufwand bekämpfen. Nur wer über den Einfluss der IT auf die Geschäftsprozesse Bescheid weiß, kann alle relevanten Risiken erkennen. *(jha)*

Merkmale eines ISMS

Ein Informationssicherheits-Management-System (ISMS)

- ist eine Aufstellung von **Verfahren und Regeln**, um die Informationssicherheit im Unternehmen zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern;
- hat eine **Sicherheitsstrategie** zum Ziel und schafft Rollen wie etwa den IT-Sicherheitsbeauftragten (auch Informationssicherheits-Beauftragter oder Chief Information Security Officer, CISO, genannt);
- betreibt **Audits** und **inventarisiert IT-Anwendungen und -Systeme**. Die IT-Installationen werden den relevanten Geschäftsprozessen zugeordnet;
- wird in der Norm ISO/IEC 27001 beschrieben. Eine erweiterte Form bieten die IT-**Grundschutz-Standards** des Bundesamts für Sicherheit in der Informationstechnik (BSI);
- bietet eine Basis für Unternehmen und Behörden, um sich nach ISO-Norm und BSI-Standard **zertifizieren** zu lassen.

***Holger Gerlach** ist Geschäftsführer von OneConsult Deutschland.