cebis
Landkreis Neu-Ulm

IT-Sicherheit durch Audit und Zertifizierung

Die Zahlen sprechen eine klare Sprache: Laut einer Cybercrime-Studie ist pro Woche mit einem erfolgreichen Angriff auf die IT-Infrastruktur zu rechnen (http://imari.dhbw-heidenheim.de/url/ct1211-01) - und das, obwohl jedes Unternehmen heute über technische Lösungen wie Virenschutz und Firewall verfügt. Da stellt sich dann doch die Frage, wie das möglich sein kann.

Betriebsblindheit

Ein sicheres Unternehmen entsteht nicht durch den Kauf eines magischen Kastens, den man einfach ins Netzwerk stellt - und das, ohne Konfigurations-Einstellungen vorzunehmen. Es bedarf vielmehr immer der richtigen und vor allem individuellen Integration in die Netzwerklandschaft des Unternehmens. Das schließt selbstverständlich Maßnahmen wie ein regelmäßiges Prüfen und Aktualisieren mit ein. Zwar sind integrierte Softwarefunktionen wie das Autoupdate sehr praktisch, aber in der Vergangenheit wurde damit so manche Sicherheitslücke nicht automatisch geschlossen, ja sogar vermeintlich bereits seit langem geschlossene Angriffspunkte wieder "nutzbar"gemacht.

Wer an die Wirksamkeit eingesetzter Hard- und Software glaubt, ohne sie jemals tatsächlich überprüft zu haben, muss schon sehr betriebsblind sein! Virenschutzprogramme und Firewalls sind Standardsoftware-Produkte; da sich aber IT-Landschaften in Unternehmen unterscheiden, müssen diese Sicherheitsprogramme daran individuell angepasst werden. Was für die eine IT-Infrastruktur ein extrem kritischer Angriffspunkt ist, ist für einen andere völlig harmlos. Das Abarbeiten von passenden Checklisten liefert zwar gute Anhaltspunkte, reicht aber nicht aus.

Technikverliebtheit

Bedauerlicherweise wird bei vielen Unternehmen IT-Sicherheit nur punktuell betrieben. Das ist nachvollziehbar, denn die "IT-vernarrten" Verantwortlichen denken gerne in technischen Systemen und Lösungen. „Nachvollziehbar“ kann aber keinesfalls heißen, dass diese Einstellung zu billigen ist. Der Erwerb eines möglichst teuren oder komplexen Stücks Hard- oder Software (oder beides zusammen als sogenannte "Appliance") beruhigt ungemein. Sicherheits-Experten (und Hacker?) entdecken in solchen Fällen aber sehr schnell die Kraftlosigkeit dieses Papiertigers. Aufeinander gestapelte Rechnungen einzelner IT-Sicherheitsinvestitionen ersetzen eben kein umsichtiges Sicherheitskonzept.

Lösung: Informationssicherheitsmanagement

Eine sichere Lösung kann immer nur in der Erfüllung beider Aspekte liegen - technisch und organisatorisch. Nicht umsonst fordert § 9 Bundesdatenschutzgesetz (BDSG) von Unternehmen dokumentierte technische und organisatorische Maßnahmen (http://www.gesetze-im-internet.de/bdsg_1990).

Investitionen in die technische IT-Sicherheit sind selbstverständlich sinnvoll und absolut notwendig - aber eben nur in Kombination mit - schriftlich fixierten -

- organisatorischen Regelungen. Beispiele: Wie halten wir es im Unternehmen mit privater IT-Nutzung von dienstlichen Geräten? Haben betriebsfremde Zugriff auf die EDV des Unternehmens? Wer archiviert wann, was, wie lange?
- abzuarbeitenden Maßnahmenkatalogen. Beispiele: Backup-Regelungen, regelmäßige interne Prüfverfahren, Einlagerung und Sicherung eigener Datenarchive.

Unterstützt wird dies sowieso durch die Neigung der Unternehmensführung, betriebliche Sachverhalte gerne schriftlich geregelt zu haben. Aber Vorsicht - mit schriftlichen Regelungen für die Schublade ist es nicht getan. Unter dem juristischen Blickwinkel ist die so genannte "betriebliche Übung" entscheidend: Wer nicht regelmäßig die Einhaltung dieser Richtlinien prüft und durchsetzt, macht sich strafbar und verliert im Schadensfall Ansprüche. Und dabei ist in der Regel das schwächste Glied der (Maßnahmen-)Kette entscheidend. Ein tragfähiges Sicherheitsniveau entsteht jedenfalls nur durch ein ganzheitliches Informationssicherheits-Management.

Externe Auditoren gegen Betriebsblindheit

Für die Planung konkreter Maßnahmen lohnt sich der Blick in die Grundschutzkataloge des Bundesamtes für Sicherheit in der Informationstechnik (BSI; http://imari.dhbw-heidenheim.de/url/ct1211-02). Der Grundschutz ist eine gute Basis, nicht mehr und nicht weniger. Auch hier gilt: Umgesetzte Maßnahmen sind durch regelmäßige Audits zu überprüfen.

Aber wer soll als Auditor prüfen? Bei internen Auditoren ist die Gefahr der Betriebsblindheit groß - insbesondere, wenn man den Bock zum Gärtner macht und die Prüfung von Mitarbeitern der eigenen IT-Abteilung durchführen lässt. Also von denjenigen, die eigentlich überprüft werden müssen. Ein externes Audit hat diese Nachteile nicht - ein neutraler Auditor kann jederzeit feststellen, ob die gewählten Maßnahmen für das angestrebte Grundschutzziel ausreichen, und im Bedarfsfall ohne Rücksicht auf scheinbare betriebliche „Sachzwänge“ und „Beziehungsgeflechte“ notwendige Maßnahmen einleiten - bevor es zum Sicherheits-Desaster kommt.

An dieser Stelle muss man sich allerdings vor Augen halten, dass ein Audit mit einer geologischen Probebohrung zu vergleichen ist und eben nur einen kleinen Ausschnitt des ausgewählten Prüf-Bereiches erfasst. Aber: Ein erfahrener Auditor hat eine „Nase“ für Problemfelder; die Wahrscheinlichkeit, dass er sich die „richtigen“ Bereiche vornimmt, ist hoch.

Normen bieten Sicherheit

Hinzu kommt, dass ein Audit immer auf eine bestimmte Sicherheitsnorm bezogen sein sollte; die Norm bestimmt, was als sicher gilt und der Auditor prüft, ob diese Normvorstellungen erfüllt sind. Hier gilt: Anerkannte internationale Sicherheitsnormen wie ISO/IEC 27001, CoBIT oder ITIL und auch anerkannte nationale Standards wie der BSI IT-Grundschutz garantieren ein Mindestmaß an IT-Sicherheit und damit auch (Datenschutz-)Rechts-Sicherheit. Selbst erfundene „Sicherheitsstandards“ von selbsternannten Auditoren sind unnütz und gefährlich!

In diesem Zusammenhang haben sich insbesondere folgende Normen in der IT-Sicherheitspraxis durchgesetzt:

- Ein Audit nach dem internationalen Standard ISO/IEC 27001 deckt beispielsweise im Bereich "Compliance" die deutschen Datenschutzanforderungen ab und bietet eine ganzheitliche Betrachtungsweise auf das, "was getan werden muss". Das "Wie" ist in dieser Norm sinnvollerweise nicht enthalten. Der Grund liegt in der Vielfältigkeit der IT-Landschaften bzw. der Unternehmensstrukturen. Interessant ist, dass die internationale Norm auch in kleinen Unternehmen umgesetzt werden kann, da sie ein schlankes Informationssicherheits-Management zulässt.
- Im Fall der BSI-Grundschutzkataloge wird die Umsetzung in kleinen Unternehmen eher schwierig, besonders auch bei Unternehmen mit völlig anderen oder stark individuellen Anforderungen an einen Basisschutz.
- Eine weitere internationale Norm, die ISO/IEC 27005, bietet ein praktisches Modell zur IT-Risikoanalyse, die als Ergebnis die IT-Sicherheitslage beschreibt und konkrete Anhaltspunkte liefert, ob der Basisschutz ausreicht oder ob noch weitere Maßnahmen selbst entwickelt werden müssen.

Goldmedaille Zertifikat

Wurde im Audit festgestellt, dass die Sicherheitsanforderungen eines Sicherheitsstandards erfüllt wurden, kann sich das Unternehmen dieses mit einem Zertifikat bescheinigen lassen. Das Zertifikat dient zur eigenen Beruhigung (zumindest bis zum nächsten Audit); es kann aber auch werbewirksam eingesetzt werden. Insbesondere bei Unternehmen, deren Kunden einen hohen Wert auf Daten- und Informationssicherheit legen (etwa bei sicherheitskritischen Produkten oder bei Online-Shops), können solche Zertifikate als Beleg für Sicherheit verwendet werden.

Die Informationssicherheit ist immer im Fluss, das heißt in relativ kurzen Abständen muss immer wieder durch ein Audit geprüft werden, ob das Konzept, die Maßnahmen und Mechanismen noch angemessen sind. Demzufolge können Checklisten, Grundschutzmaßnahmen oder Benutzerrichtlinien von gestern ein Unternehmen von heute unsicher machen, obwohl man mit Überzeugung alle Punkte schon mal abgehakt hat. Der größte Feind der Informationssicherheit ist also nicht der Aufwand, sondern die Schein-Sicherheit.

Gerade im Bereich Datenschutz müssen sich übrigens Unternehmen in den nächsten Jahren auf häufigere Audits einstellen. Da auch jedes externe Audit immer interne Ressourcen belastet, ist es grund-

sätzlich ratsam, über eine entsprechende ganzheitliche Zertifizierung nachzudenken, die dann künftige Audit-Anfragen in Minutenschnelle erledigbar macht.

Zu teuer für KMU?

Kein Unternehmen ist zu klein oder zu unwichtig für Informationssicherheit. Daher sollten auch kleinere und mittelgroße Unternehmen (KMU) bei diesem Thema nicht den Kopf in den Sand stecken - bei Verstößen gegen den Datenschutz und bei Verlust von wichtigen Betriebsgeheimnissen könnte es sonst sein, dann man den Kopf aus dem Sand nicht mehr heraus bekommt.

Selbstverständlich entstehen durch Sicherheitsmaßnahmen und Audits Kosten, die nicht unmittelbar in Umsatz münden. Aber eine verantwortungsvolle Unternehmensführung bewertet die Risiken durch die eigene IT und stellt sie den Aufwendungen für Sicherheitsmaßnahmen gegenüber - und erkennt dabei sehr schnell die Notwendigkeit, IT-Sicherheit zu gewährleisten.

CEBIS hilft weiter

Unternehmen, die Informations- und Beratungsbedarf zu Chancen, aber auch Risiken von IT und Internet haben, können sich an CEBIS wenden. Informieren Sie sich auf der CEBIS-Website und melden Sie Ihren Beratungsbedarf möglichst frühzeitig an.

Tipp des Monats November 2012