tierenden Folgen wie Wirtschaftsspionage und -kriminalität, aber auch vor Sabotage sowie ungewolltem Datenabfluss zu schützen.
Hundertprozentige Sicherheit gibt es nicht, aber es ist doch möglich, die unternehmenskritischen Informationen optimal abzusichern. Hierfür muss die IT-Sicherheit als kontinuierlicher Prozess betrachtet werden, der über den Basisschutz hinausgeht. So ist die Implementierung der standardmäßigen Sicherheitslösungen wie Firewall und Virenscanner zwar ein unabdingbares Muss, aber eben nur das absolute Minimum, welches mittlerweile allerdings nicht mehr ausreicht.
Doch wie kann die bestmögliche Absicherung erfolgen? Empfehlenswert, weil in der Praxis bewährt, um das Sicherheitsniveau im Unternehmen den Erfordernissen anzupassen, ist eine graduelle Vorgehensweise. Dies bedeutet, alle Maßnahmen – sowohl technische, organisatorische als auch rechtliche – in einem ganzheitlichen IT-Sicherheitskonzept zusammenzufügen. Im Rahmen der Strategieentwicklung gilt es also, im ersten Schritt die schützenswerten Daten zu ermitteln sowie darauf aufbauend die entsprechenden Prozesse und Maßnahmen zu definieren.
Auf diesen Informationen basiert der Stufenplan, an dessen Anfang die Definition eines verbindlichen Regelwerks für die Sicherheit im Unternehmen steht und im Weiteren dann die Planung und Umsetzung der konkreten Schutzmaßnahmen.
Oberste Priorität sollte sein, ein – unter Kosten-/Nutzenaspekten – jeweils angemessenes Schutzniveau für jede Abteilung und alle Daten zu projektieren. Denn eine undifferenzierte Vorgehensweise birgt hier die Gefahr, dass die Sicherheitsmaßnahmen partiell zu umfangreich und damit zu teuer ausfallen, auf der anderen Seite jedoch für besonders schützenswerte Bereiche wie etwa die Forschungs- und Entwicklungsabteilung oder die hochsensiblen (unternehmenskritischen) Informationen zu gering dimensioniert wären.

Wolfgang Straßer, Geschäftsführer der @-yet GmbH, Pulheim

Tipps – wo dringend etwas getan werden muss

1) Geschäftsleitung/Organisation

- Die Geschäftsleitung muss die Bedeutung der IT als Träger wertvoller Unternehmenswerte anerkennen und entsprechend die Priorität der IT-Sicherheit hoch genug ansetzen.
- Die Inventarisierung der Unternehmenswerte ist der Grundstein, um die eingesetzten Maßnahmen an den tatsächlichen Schutzbedarf anzupassen.
- Es bedarf ausformulierter Sicherheitsrichtlinien.

2) Technik

- Bei der Einführung neuer Technologien ist deren Absicherung in ausreichendem Maße zu berücksichtigen.
- Die üblichen Standards wie Virenscanner und Firewall reichen nicht aus.
- Mobile Endgeräte müssen zwingend in der Sicherheitsstrategie berücksichtigt werden, inklusive entsprechender Sicherheitskonzepte wie etwa VPN.

Foto: gunnar 3000, fotolia.com

3. Tag der IT-Sicherheit

14. Juli 2011, 14–18.30 Uhr, im IHK Haus der Wirtschaft in Karlsruhe

Der Tag der IT-Sicherheit zeigt in diesem Jahr zum dritten Mal aktuelle IT-Sicherheitsbedrohungen für Unternehmen auf. Er macht deutlich, wie wichtig ein professioneller Umgang mit dem Thema IT-Sicherheit ist, und informiert ausführlich zu Präventionsmöglichkeiten.

14.00 Uhr **Begrüßung**
Bernd Bechtold, Präsident der Industrie- und Handelskammer Karlsruhe
Moderation: Dirk Fox, Mitinitiator der Karlsruhe IT-Sicherheitsinitiative (KA-IT-Si) und Vorstand im CyberForum e. V.

14.10 Uhr **Keynote: Die Perspektive der IT-Sicherheit in Deutschland und die Rolle des BSI**
Michael Hange, Präsident des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

14.45 Uhr **De-Mail**
Sven Gelzhäuser, Product Manager De-Mail, 1&1 Mail & Media GmbH

15.30 Uhr **Elektronischer Personalausweis**
Jens Fromm, Leiter der Forschungsgruppe Elektronische Identitäten, Fraunhofer FOKUS

16.15 Uhr **Pause und Networking mit Ausstellung**

17.00 Uhr **Web-Angriffe: Echte Zauberei oder billige Tricks?**
Kai Jendrian und Klaus J. Müller, Secorvo Security Consulting GmbH

17.45 Uhr **Sicherheit im Online-Banking**
Lutz Bleyer, Leiter der Stabsabteilung Zentrale Security, FIDUCIA IT AG

18.30 Uhr **Jubiläumsempfang anlässlich des 10-jährigen Bestehens der Karlsruher IT-Sicherheitsinitiative**

Informationen
Telefon (07 21) 174-438
christina.pieck@karlsruhe.ihk.de

liegen und die Persönlichkeitsrechte von Nichtbetroffenen strikt beachtet werden. Bei der Einschleusung muss neben der Zustimmung des Auftraggebers auch die des Betriebsrats gegeben sein.

Qualitätsstandards

Da der Gesetzgeber keine fachlichen Qualitätsnachweise für die Aufnahme einer Detektivtätigkeit fordert, sieht sich der Bundesverband Deutscher Detektive in der selbst auferlegten Verpflichtung, dafür zu sorgen, dass stets qualitativ hochwertige Dienstleistungen angeboten werden. Diesem Zweck dienen die seit dem Jahr 1957 jährlich stattfindenden Fortbildungsseminare des Verbandes. Die Themen dieser Seminare werden weitestgehend von den Wünschen der Mitglieder bestimmt und sind darauf ausgerichtet, einen stets aktuellen Kenntnis- und Wissensstand zu gewährleisten.

Um auch die durch die Europäische Richtlinie 2005/36/EG über die Anerkennung von Berufsqualifikationen bedingten steigenden qualitativen Anforderungen auch künftig europaweit erfüllen zu können und der Forderung, insbesondere aus der Wirtschaft, nach überprüfbarer Qualität detektivscher Dienstleistungen gerecht zu werden, hat der BDD auf seiner 59. Jahreshauptversammlung am 16. Mai 2009 ein Qualitätssicherungskonzept für detektivische Dienstleistungen beschlossen. Mit diesem Qualitätssicherungskonzept soll eine klare und eindeutige Orientierungsgrundlage für die Wirtschaft, aber auch für den einzelnen Verbraucher, im Hinblick auf die Vergabe von detektivischen Aufträgen zur Verfügung gestellt werden.

Der Bundesverband Deutscher Detektive wird auch in Zukunft trotz der sich rasant verändernden Bedingungen alles tun, um seiner sich selbst auferlegten Verpflichtung, permanent hochwertige Dienstleistungen sicherzustellen, gerecht zu werden. Außerdem wird es in nächster Zeit sein Bestreben sein, das von ihm entwickelte Qualitätssicherungskonzept für detektivische Dienstleistungen in Deutschland auf eine breite Grundlage zu stellen.

Eveline Wippermann, Präsidentin des Bundesverbandes Deutscher Detektive, Bielefeld

[www.bdd.de]

Es gibt im Bereich der Wirtschaftskriminalität kein Deliktfeld, auf dem Detektive nicht erfolgreich tätig sind, so zum Beispiel bei Verletzung des Patent- und Markenrechts.

Foto: René Spruth, fotolia.com

Foto: N Media, fotolia.com

Sichere Software

Viele IT-Sicherheitsvorfälle und Datenverluste haben ein und dieselbe Ursache: sicherheitskritische Fehler in Programmen oder Betriebssystemen, die von einem Hacker oder einem zum Beispiel per E-Mail verbreiteten Schadprogramm ausgenutzt wurden.

Will man nicht nur mit Virenschutzprogrammen lediglich die Auswirkungen der Symptome erreichen, sondern das Übel an der Wurzel packen, bleibt nur ein einziger Weg: Die Entwicklung von Software ohne Sicherheitslücken, auch als „sichere Softwareentwicklung" bezeichnet.

Das ist leichter gesagt als getan – und das nicht nur, weil fehlerfreie Software an sich bereits eine große Herausforderung darstellt. Erschwerend kommt hinzu, dass auch gute Programmierer häufig keine Kenntnis von typischen sicherheitskritischen Programmierfehlern haben – und daher oft die Fehler anderer wiederholen. Auch die Zunahme von über das Internet erreichbaren Anwendungen (Shop-Systeme, Online-Dienste) verschärft das Problem: Mehr potenzielle Angreifer erhöhen das Risiko, dass eine Schwachstelle auch gefunden wird. Zudem neigen Entwickler von Web-Anwendungen dazu, anders als bei klassischer Softwareentwicklung, häufiger Änderungen an der Software vorzunehmen – oft sogar unter Verzicht auf eine Test- und Abnahmephase.

Der wichtigste Faktor bei der Entwicklung sichererer Software ist die Erweiterung des Softwareentwicklungs- und Freigabeprozesses um zusätzliche, auf die Sicherheitseigenschaften der Software fokussierte Schritte. Dazu gehören Testfälle, die die Anfälligkeit der Software für bekannte Angriffe wie beispielsweise Cross Site Scripting prüfen, (externe) Reviews, die das System auf konzeptionelle Fehler hin untersuchen (wie fehlerhafte Sicherheitsprotokolle) und abschließende Penetrationstests.

Wesentliche Voraussetzung dafür, dass sich ein solcher, stärker an Sicherheitsaspekten orientierter Prozess durchsetzt, ist jedoch die Sensibilisierung und Schulung der Entwickler für die Bedrohung durch und die wirksame Vermeidung von Sicherheitslücken. Mehr zum Thema IT-Sicherheit von Web-Anwendungen sind auf der Internetseite der OWASP (Open Webapplication Security Project)-Organisation zu finden.

Petra Barzin, Secorvo Security Consulting GmbH, Karlsruhe

Informationen

Telefon (07 21) 174-438
christina.pieck@karlsruhe.ihk.de
www.owasp.org