Elektronische Sicherung von Gebäuden >
< Sicherheitsmaßnahmen für Unternehmen

Informationssicherheit im Unternehmen

Von »Antivirenschutz« bis »Sichere Zugangsdaten«

Informationssicherheit kommt häufig zu kurz

Bei der Gebäudesicherung eines Unternehmens kommt der Bereich Informationssicherheit häufig zu kurz. Aus Unwissenheit oder Kostengründen wird auf wichtige Investitionen verzichtet. Welche schwerwiegenden Folgen dies haben kann, macht sich oft erst im konkreten Schadensfall bemerkbar – wenn etwa durch mangelnde Datensicherung wichtige Unterlagen verloren gehen oder ein Computervirus das ganze Firmennetzwerk lahm legt. Beim Thema Informationssicherheit geht es jedoch nicht nur um die Sicherung von Computern. Holger Schildt vom Bundesamt für Sicherheit in der Informationstechnik (BSI)

Die häufigsten Fehler und die wichtigsten Schutzmaßnahmen rund um Informationssicherheit in Unternehmen:

1. Unzureichende Informationssicherheitsstrategie
Schutzmaßnahmen:

- Informationssicherheitsaspekte müssen etwa bei der Anschaffung einer neuen Software von vornherein berücksichtigt werden. Abstriche beim Komfort oder der Funktionalität zugunsten der Sicherheit zahlen sich in der Regel aus!
- Es müssen Sicherheitsziele definiert werden: Welche Informationen sind konkret zu schützen? Know-how, Betriebsgeheimnisse, personenbezogene Daten oder IT-Systeme? Daraus müssen passende

- Maßnahmen abgeleitet werden, die regelmäßig mit den Sicherheitszielen abgeglichen werden.
- Bei jeder Sicherheitsmaßnahme muss festgelegt werden, wer diese wann und wie häufig durchführt – etwa die Aktualisierung von Virenschutzprogrammen.
- Sicherheitsrichtlinien und Zuständigkeiten müssen allen Mitarbeitern bekannt sein. Jeder Mitarbeiter sollte wissen, worauf er achten muss und an wen er sich bei Fragen zur Informationssicherheit wenden kann.
- Die Informationssicherheit im Unternehmen muss regelmäßig überprüft werden – wenn das Budget es zulässt, am besten einmal jährlich durch unabhängige Experten. Es muss hinterfragt werden: Sind Sicherheitsrichtlinien veraltet, unvollständig oder nicht praktikabel?
- Alle bestehenden Sicherheitsrichtlinien sollten schriftlich dokumentiert werden.

2. Schlechte Konfiguration und Wartung von IT-Systemen / mangelnde Nutzung von vorhandenen Sicherheitsmechanismen

Schutzmaßnahmen:

- Sicherheitsupdates müssen regelmäßig und zeitnah eingespielt werden. Dies gilt nicht nur für Virenschutzprogramme, sondern für sämtliche genutzte Software wie beispielsweise Web-Browser oder E-Mail-Programme und für das Betriebssystem. Dazu müssen Routinen eingerichtet und Verantwortlichkeiten festgelegt werden.
- Jeder Mitarbeiter und Administrator sollte nur auf die Daten zugreifen und die Programme ausführen können, die er für seine Arbeit benötigt. Es sollte regelmäßig überprüft werden, ob die eingeräumten Rechte noch seiner Tätigkeit entsprechen.
- In vielen Programmen sind bereits Schutzmechanismen integriert – diese müssen jedoch richtig konfiguriert werden. Standardeinstellungen wie etwa Passwörter müssen angepasst bzw. geändert werden. Dies gilt auch für komplette vorkonfigurierte IT-Systeme oder Telekommunikationsanlagen.

3. Unsichere Vernetzung und Internet-Anbindung Schutzmaßnahmen:

- Aktuelle Virenschutzsoftware ist ein absolutes Muss sowohl für Rechner als auch für mobile Geräte wie Notebooks.
- Schützen Sie Ihr Firmennetz mit einer geeigneten und entsprechend konfigurierten Firewall gegen Angriffe aus dem Netz.
- In größeren Unternehmen sollten Teilnetze aufgebaut werden, die jeweils gegen die benachbarten Netze durch spezielle Firewalltypen geschützt sind.
- WLAN-Netze dürfen nur verschlüsselt genutzt werden.
- Server und zentrale Rechner müssen „gehärtet“ werden. „Härten“ bedeutet, dass sich keinerlei Software auf dem Rechner/Server befindet, die dort nicht zwingend benötigt wird.
- Nach außen angebotene Daten, Dienste und Programme sollten auf das Mindestmaß beschränkt werden.
- Im Web-Browser sollten nur die Aktiven Inhalte und Multimedia-

Der ausführliche „Leitfaden Informationssicherheit – IT-Grundschutz kompakt“ steht auf der BSI-Webseite als PDF-Dokument zum kostenfreien Download zur Verfügung [PDF] https://www.bsi.bund.de/

- PlugIns zugelassen werden, die für die Arbeit wirklich benötigt werden. ActiveX-Komponenten stellen eine Gefahr dar und sollten möglichst deaktiviert werden. Welche Skripte, Protokolle oder Zusatzprogramme gemieden werden sollten, kann sich im Laufe der Zeit ändern. Administratoren können sich über die Webseiten des BSI über aktuelle riskante Techniken informieren.
- Schadprogramme werden häufig über E-Mail-Anhänge verbreitet. Mitarbeiter sollten daher keinesfalls unbedacht Anhänge öffnen und ausführen. Das genutzte E-Mail-Programm sollte so konfiguriert werden, dass Anhänge nicht automatisch geöffnet werden.
- Wenn möglich, sollten Sicherheitsmaßnahmen technisch erzwungen werden, damit das Risiko einer Fehlbedienung oder absichtlich herbeigeführten Schadens minimiert werden kann.
- Auch erfahrene Administratoren sollten stets die Handbücher zu den eingesetzten Produkten lesen, damit spezielle Warnhinweise nicht übersehen werden. Außerdem sollten ausführliche Installations- und Systemdokumentationen angefertigt werden, die auch von Dritten nachvollzogen werden können.

4. Nichtbeachtung von Sicherheitsmaßnahmen Schutzmaßnahmen:

- Die konsequente Beachtung aller Sicherheitsregeln ist für die Informationssicherheit in einem Unternehmen unerlässlich.
- Alle Mitarbeiter in einem Unternehmen sollten ein Grundverständnis für Informationssicherheit haben und Gefahren einschätzen können.
- Ordnung am Arbeitsplatz ist ein Teil der Informationssicherheit: Vertrauliche Akten, Datenträger mit sensiblen Informationen wie CDs oder USB-Sticks sollten nie offen herumliegen, sondern bei Verlassen des Raumes weggeschlossen werden. Sollen sensible Daten entsorgt werden, müssen diese unwiederbringlich vernichtet werden: Vertrauliche Ausdrucke gehören in den Aktenvernichter, nicht in den Papierkorb. Datenträger müssen sicher gelöscht oder zerstört werden.
- Datendiebe könnten versuchen, über Social Engineering-Techniken – etwa über das Telefon oder per E-Mail – an vertrauliche Unternehmensdaten zu gelangen. Mitarbeiter müssen dafür sensibilisiert werden.
- Administratoren müssen sich stetig fortbilden, Mitarbeiter müssen für Fragen der Informationssicherheit sensibilisiert und regelmäßig geschult werden. Dies kann über interne Vorträge, Schulungen, Rundschreiben, Plakate etc. geschehen. Konkrete Handlungsanweisungen sind hier wichtig, zum Beispiel darüber, welche konkreten Informationen nicht an Dritte weitergegeben werden dürfen. Passwörter dürfen nicht in der Schreibtischschublade aufbewahrt werden. Bei Verlassen des Büros müssen die Fenster geschlossen werden. Anschauliche Beispiele erhöhen das Verständnis und die Akzeptanz.
- Werden Wartungen oder Reparaturen im Unternehmen durchgeführt, sollten Servicetechniker nie ohne Aufsicht an IT-Systemen oder Telekommunikationsanlagen arbeiten.
- Sicherheitsverstöße im Unternehmen sollten Konsequenzen nach sich ziehen und angemessen sanktioniert werden.
- Informationssicherheit gilt auch für unterwegs: Wird etwa im Zug mit dem Notebook gearbeitet,

- sollten sensible Daten nicht für Dritte einsehbar sein. Bei Telefongesprächen in der Öffentlichkeit muss ebenfalls auf Diskretion geachtet werden. Offene WLAN-Netze sollten nicht genutzt werden.

5. Sorgloser Umgang mit Passwörtern Schutzmaßnahmen:

Sensible Daten sollten verschlüsselt werden

- Es müssen sichere Passwörter gewählt werden, das heißt, sie müssen gewissen Qualitätsanforderungen genügen: Ein Passwort sollte länger als sieben Zeichen sein, nicht im Wörterbuch vorkommen, nicht aus Namen bestehen und neben Groß- und Kleinbuchstaben auch Sonderzeichen und Zahlen beinhalten.
- Passwörter sollten regelmäßig ausgetauscht werden. Außerdem sollte ein und dasselbe Passwort nie für mehrere Dienste/Accounts eingesetzt werden.
- Die oben genannten Sicherheitsmaßnahmen machen es nicht einfach, sich Passwörter zu merken. Es ist daher legitim, Passwörter zu notieren. Diese sollten aber unbedingt an einem sicheren Ort aufbewahrt werden (dazu gehören nicht der Monitor oder die Schreibtischschublade).
- Voreingestellte Passwörter von Programmen oder Software sollten geändert werden.
- Jeder Rechner sollte beim Verlassen des Arbeitsplatzes mit Bildschirmschoner und Passwort gesichert werden.
- Es ist sinnvoll, sensible Daten mit einer Verschlüsselungssoftware zu schützen. Notebooks oder andere mobile Geräte sollten komplett verschlüsselt werden.

6. Mangelhafter Schutz vor Einbrechern und Elementarschäden Schutzmaßnahmen:

Das bayerische Landesamt für Verfassungsschutz bietet auf seiner Webseite einen virtuellen Rundgang durch ein Unternehmen an und zeigt konkrete Schwachstellen rund um die Informationssicherheit auf: www.wirtschaftsschutz-bayern.de.

- Es sollten Notfallpläne entwickelt werden, damit jeder Mitarbeiter weiß, was bei einem konkreten Vorkommnis zu tun ist: Wer sorgt etwa dafür, dass Systeme wiederhergestellt werden? Wie wird ein Backup zurückgespielt?
- IT-Systeme müssen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt werden. Achtung: Hier muss es sich nicht gleich um große „Katastrophen“ handeln: Auch ein umgekippter Putzeimer kann schon viel Schaden anrichten.
- Alle wichtigen Daten müssen regelmäßig gesichert werden – auch die Daten auf Notebooks oder Smartphones. Es muss regelmäßig überprüft werden, ob das Backup funktioniert und die gespeicherten Daten erfolgreich wieder eingespielt werden können.
- Backups müssen an einem sicheren Ort aufbewahrt werden –

- am besten außerhalb des Unternehmens. Am Aufbewahrungsort sollten Maßnahmen gegen Feuer- und Wasserschäden usw. getroffen werden.
- Es sollten Einbruchschutzmaßnahmen und ggf. Zutrittskontrollen umgesetzt werden. Besucher, Handwerker etc. sollten bei ihren Aufenthalten im Unternehmen beaufsichtigt werden.
- Arbeiten Mitarbeiter extern mit Notebooks oder Smartphones, ist auch hier auf die Sicherheit zu achten: Notebooks sollten beispielsweise nie im Auto liegengelassen werden.

Folgende Artikel könnten Sie auch interessieren:

Sicherheitskonzept für das eigene Unternehmen
Elektronische Sicherung von Gebäuden
Neue Wege im gewerblichen Brandschutz

Alle Artikel dieser Kategorie

Weitere Infos zum Thema gewerbliche Gebäudesicherheit

Verhaltensfehler führen zu Sicherheitsmängeln in Unternehmen

Sicherheitsrisiko Mensch

„Wie schütze ich meinen Betrieb vor Einbruch und Datendiebstahl?“ Mit...[mehr erfahren]

So schützt man sich am besten

Wie Einbrecher vorgehen

Heinrich Hauner ist Kriminalhauptkommissar beim Präsidium München....[mehr erfahren]

Die Videoüberwachung von Betriebsgebäuden ist nur unter bestimmten Bedingungen sinnvoll – und erlaubt

Vorsicht Kamera!

Einbruchsgefahr, Diebstähle durch Supermarktkunden, Unterschlagungen...[mehr erfahren]

Mit Peter Werkmüller, Polizeiliche Beratungsstelle Düsseldorf

Video: Einbruchschutz in Gewerbeimmobilien

In diesem Video befasst sich Hauptkommissar Peter Werkmüller von...[mehr erfahren]

Diagnose: Hohe Einbruchsgefahr

Sicherheit in Arztpraxen

Arztpraxen sind in Deutschland seit der Einführung der Praxisgebühr...[mehr erfahren]