Fast Facts:

- Der optimale Weg für IT-Security im Unternehmen erfordert, dass Sicherheit bei allen Prozessen ein Thema ist
- Oft wird Sicherheit aber aus Zeit- und Budgetgründen zunächst zurückgestellt
- Sicherheitsüberlegungen kommen erst im Nachgang
- Der Artikel bietet eine Checkliste, wie Unternehmen das Risiko dabei minimieren können.
- **Zeichen: 7714 mit Leerzeichen**

Wenn IT-Sicherheit im Unternehmen konsequent gelebt wird, dann muss sie bei allen Prozessen und Entscheidungen ein Thema sein. In der Praxis ist das aber oft nicht der Fall, dann werden etwa neue Programme, Dienste und Geräte genutzt und die Sicherheit kommt erst im Nachgang auf den Tisch. Der Artikel zeigt, wie man die entstehenden Risiken minimieren kann.

Sicherheit im Nachgang

In vielen Unternehmen wird IT-Sicherheit vernachlässigt. Erst werden neue Geräte, Software und Dienste eingeführt und später wird über deren Schutz nachgedacht. Mit der passenden Strategie kann man das Risiko dabei minimieren.

Die richtige Vorgehensweise bei IT-Security im Unternehmen sieht so aus: Sicherheit ist nicht nur ein Anhängsel oder eine Überlegung, die man ab und zu anstellt. Bei allem, was im Unternehmen passiert, muss das Thema IT-Sicherheit berücksichtigt werden. Ein Beispiel: Wenn der Geschäftsführer ganz plötzlich eine Begeisterung für Tablet-Computer entwickelt und diese als zusätzliches Arbeitsgerät nutzen möchte, dann muss das Sicherheitskonzept so erweitert werden, dass das Arbeiten auf den mobilen Geräten auch den Sicherheitsrichtlinien des Unternehmens genügt. Alle Änderungen an der IT sollten vorher hinterfragt werden und erst, wenn sie ins Security-Konzept passen, umgesetzt werden. Soweit die Theorie, in der Praxis sieht das vielfach anders aus. Schuld sind wie so oft knappe Budgets und die dünne Personaldecke. Dann passiert es

eben, dass der Chef mit dem iPad in der Hand den Administrator drängelt und für Sicherheit erst einmal keine Zeit bleibt. Doch es stimmt auch nicht, dass sich Unternehmen gar nicht um IT-Sicherheit kümmern, meist tauchen die Fragen zur Absicherung aber erst im Nachgang auf, also wenn neue Software und Dienste bereits implementiert sind oder die mobile Hardware an die Mitarbeiter ausgegeben wurde. Mit der passenden Strategie schaffen Sie es, das Risiko dabei zu minimieren.

Alle Unternehmen sind betroffen

Wichtig ist, dass sich zumindest die Firmen selbst der Gefahr durch IT-Bedrohungen bewusst sind. Unternehmen jeder Größenordnung können Opfer von Cyberkriminellen werden. Denn auch kleine Unternehmen setzen die gleichen Tools ein wie große Firmen, beispielsweise meist Windows auf dem Desktop und Server, Internet Explorer oder Firefox als Browser, dazu ein Office-Paket und zusätzlich noch die ein oder andere Business-Software, beispielsweise um Kundendaten zu speichern. Realistische Bedrohungen für Unternehmen sind unter anderem: Diebstahl von Kunden- oder Finanzdaten, Manipulation von Überweisungen, Infektion von Workstations und Servern, Mitschneiden von Netzwerkverkehr oder Speichern von illegalen Inhalten auf Firmen-Servern.

To-Dos für Firmen

Aber was kann man jetzt konkret als kleines oder mittelständisches Unternehmen tun? Als Firma muss man sich als erstes darüber im Klaren sein, was man genau schützen will. Das ist je nach Unternehmen unterschiedlich und deshalb gibt es auch keine One-fits-all-Strategie zum Schutz. Folgende Checkliste können aber alle Unternehmen abarbeiten, die ihr IT-Risiko minimieren wollen:

1. Mitarbeiter sensibilisieren: Sie selbst und Ihre Mitarbeiter müssen misstrauisch sein. Was zu schön ist, um wahr zu sein, ist üblicherweise auch nicht wahr. Wenn Ihnen ein Lieferant plötzlich seine Ware für ein Zehntel des üblichen Preises anbietet, werden Sie auch hellhörig. Gleiches gilt natürlich auch für Mails, Messenger oder Mitteilungen in sozialen Netzwerken. Aber auch bei scheinbar ungefährlichen Aktionen im Internet ist Vorsicht geboten. Beispielsweise versuchen Malware-Autoren die Suchergebnisse von Google zu manipulieren oder platzieren Ihre Schädlinge auf an sich seriösen Webseiten. Tipp: Führen Sie regelmäßig Schulungen für Mitarbeiter durch, in denen

aktuelle Sicherheitsprobleme angesprochen werden, beispielsweise beim Umgang mit sozialen Netzwerken.

2. Bewährten Schutz nutzen: Auch bei IT-Schutz gilt, suchen Sie sich bezahlbare und bewährte Technik. Wer sich selbst informieren will, findet in vielen Fachzeitschriften Tests von Sicherheits-Software. Auch viele Systemhäuser können Ihnen einen guten Überblick über erhältliche Schutz-Software und deren Leistungsfähigkeit geben. Auch bei den Sicherheitsfirmen direkt gibt es kompetente Ansprechpartner, die Ihnen im Detail erklären können, was die vorhandenen Schutzlösungen können.

3. Einfache Lösungen finden: Es gibt viele Anbieter und viele Lösungsmöglichkeiten für Sicherheitsfragen. Tipp: Nutzen Sie Sicherheitslösungen, die einfach in der Bedienung sind. So ist beispielsweise eine zentrale Management-Oberfläche, mit der alle Computer schnell verwaltet werden können, eine nützliche Sache. Gibt es vielleicht sogar schon Verwaltungs-Werkzeuge für die PCs und Server im Unternehmen, dann ist es ein Vorteil, wenn sich dort auch die Sicherheitseinstellungen integrieren lassen.

4. Komplettpakete nutzen: IT-Schutz sollte aus mehreren Modulen Bestehen. Neben Anti-Malware brauchen Sie auch Schutz vor Spionageprogrammen, Phishing-Filter und Firewall. Auch ein Intrusion Prevention Modul ist sinnvoll, um Einbrüche ins Netzwerk wirksam zu verhindern. Alle diese Komponenten sollten aber nahtlos zusammenspielen. Deshalb raten wir zu einer Komplettlösung. Denn wer zu viele einzelne Module von unterschiedlichen Herstellern kombiniert, hat damit erhöhten Aufwand und erfährt Reibungsverluste.

5. Umfassende Lösungen integrieren: Sie haben in der Mehrzahl Windows-Workstations, Windows-Server und ein paar Macs? Dann sollten Sie eine Schutzlösung wählen, die auf all diesen Systemen läuft. Wichtig auch: Wer Smartphones für Unternehmenszwecke nutzt, sollte auch die mobilen Alleskönner in die Schutzstrategie integrieren.

6. Grundschutz am PC einrichten: Vernachlässigen Sie den PC-Grundschutz nicht. Statten Sie alle Systeme mit Virenschutz und den oben genannten Zusatzmodulen aus. Richten Sie ein Patch-Management-System ein, um die komplette Software-Palette

immer auf dem aktuellen Stand zu halten. Für die Windows-Rechner reicht es beispielsweise in kleinen Unternehmen schon aus, wenn man die automatischen Updates aktiviert. Ab zehn PCs ist ein eigener Update-Server die wirtschaftlichere Lösung. Neben dem Betriebssystem müssen Sie auch alle eingesetzten Programme aktuell halten, beispielsweise Office oder das ERP-System.

7. Admin als Ausnahme verwenden: Arbeiten Sie nicht ständig mit Administratorrechten am Computer, sondern nur, wenn Sie die PCs warten oder Software installieren. Für die täglichen Arbeiten sollte jeder Nutzer nur ein eingeschränktes Benutzerkonto haben. Das ist deshalb wichtig, weil eingeschlichene Schädlinge häufig die Rechte des aktuell angemeldeten Users nutzen. Sind diese nur eingeschränkt, hat die Malware eine geringere Chance zur Weiterverbreitung.

8. Regelmäßige Backups machen: Sicherheit in der IT ist mehr als die Verteidigung gegen Malware und Hacker, auch Datensicherheit gehört dazu. Deshalb sind regelmäßige Backups Pflicht. Auch hier gilt: Eine allgemeine Strategie, die für jede Firma anwendbar ist, gibt es nicht. Unternehmen müssen erst identifizieren, welche Daten wie wichtig sind und mit diesen Erkenntnissen einen Backup-Plan einrichten. Wichtige Dokumente kann man beispielsweise sogar mehrmals täglich sichern. Bei der Mail-Datenbank reicht aber oft auch schon eine Datensicherung über Nacht. Mit Backups minimieren Sie beispielsweise den Schaden, der durch Hardware-Defekte entsteht.

9. Nur ausgesuchte Software nutzen: Die Unternehmens-PCs sollten nur mit der nötigen Software ausgestattet sein. Jedes zusätzliche Programm bietet nämlich eine unnötige Angriffsfläche. Machen Sie auch den Mitarbeitern klar, dass es ein Sicherheitsproblem ist, wenn selbst Programme installiert oder vom USB-Stick ausgeführt werden.

10. Richtlinien festlegen: Unternehmens-PCs sind in erster Linie zum Arbeiten da. Privat Surfen ist also erst einmal tabu. Viele Firmen tolerieren es aber beispielsweise, wenn Mitarbeiter in der Pause private E-Mails abrufen. Wichtig: Halten Sie in einer Richtlinie fest, was an privater Internet-Nutzung erlaubt ist und was nicht.

Other useful links:
www.securelist.com/en/analysis
www.kaspersky.com