Fast Facts:

- Der aktuelle IT-Schutzstatus vieler Unternehmen lässt zu wünschen übrig
- In 30 Prozent der Unternehmen fehlt es schon an den Grundlagen, denn dort ist nicht einmal der Malware-Schutz komplett umgesetzt
- Der Artikel erklärt, was man beim Grundschutz beachten sollte und wie man darauf weitere Sicherheitsfunktionen aufbaut.
- **Zeichen: 8.801 inkl. Leerzeichen**

Die IT-Sicherheit lässt in vielen Unternehmen noch zu wünschen übrig. Fast in jedem dritten Unternehmen fehlt es sogar noch an den grundlegendsten Schutzfunktionen. Der Artikel zeigt, was man für den IT-Grundschutz braucht und wie man darauf noch wirksamere Sicherheits-Funktionen aufbaut.

Unternehmen vernachlässigen Grundschutz

Erschreckend, manchmal fehlen in Unternehmen selbst die einfachsten IT-Sicherheitsmaßnahmen. So sind bei rund 30 Prozent der Firmen nicht einmal alle Computer mit Virenschutz ausgestattet. Der Artikel zeigt, wie man ohne großen Aufwand den Grundschutz einrichtet und darauf verbesserte IT-Sicherheitstechniken aufbaut.

Wie wichtig IT-Sicherheit ist, ist noch längst nicht in allen Unternehmen angekommen. Nach einer weltweiten Umfrage von Kaspersky ist in 30 Prozent der Unternehmen noch nicht einmal der grundlegende Malware-Schutz komplett implementiert. In der Praxis bedeutet das: Die Firmen nutzen zwar oft Virenscanner, aber entweder fehlen wichtige Module wie Anti-Spyware oder es sind längst nicht alle Computer mit Malware-Schutz ausgestattet. Beispielsweise schützen viele Unternehmen zwar ihre Windows-Desktops, die Macs in der Grafikabteilung oder die eingesetzten Smartphones besitzen aber keinen Schutz. Auch Altsysteme werden oft schutzlos weiter genutzt, weil die eingesetzte Sicherheits-Software diese Systeme nicht mehr unterstützt und gern wird auch bei den Servern im Intranet am Virenschutz gespart.

Unbedingt gegensteuern

Doch das ist keine gute Strategie, Unternehmen sollten keinesfalls auf den Grundschutz verzichten. Der ist ein absolutes Muss, wie der Sicherheitsgurt im Auto oder der Sturzhelm für den Motorradfahrer. Mit Annahmen wie "uns wird schon nichts passieren" oder "Hacker interessieren sich doch nicht für kleine Unternehmen" erleidet man leicht Schiffbruch. Folgende Komponenten gehören zu einem soliden Grundschutz:

Aufgebohrter Virenschutz für PCs

Statten Sie alle Systeme mit Virenschutz aus. Neben dem Erkennen von Viren sollte die Sicherheitslösung aber auch Spyware ausfiltern, Keylogger und Rootkits aufspüren und den Nutzer auch im Internet vor Drive-by-Downloads schützen. Eine gute Idee ist es auch, die Workstations mit einer Desktop-Firewall auszustatten.

Updates für Betriebssystem und Anwendungen

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.

Mitarbeiter-PCs schützen

Trotz rund 90 Prozent Marktanteil für Windows sollte man den Rest, also etwa Macs in der Grafikabteilung oder Linux-PCs der Entwickler, nicht ungeschützt lassen. Verwenden Sie eine Security-Software, die auf allen Betriebssystemen läuft. Der Vorteil: So lässt sich Komplexität gezielt reduzieren. Statt mehrere Lösungen unterschiedlicher Hersteller zu kombinieren, bieten Kombiprodukte, die alle Systeme schützen, viele Vorteile. So ist man in der Wahl der Plattform als Unternehmen nicht eingeschränkt. Eine Security-Lösung, die beispielsweise nur Windows als Fileserver-Betriebssystem unterstützt, würde die preiswerten Linux-Netzwerkspeicher aus dem Unternehmen verbannen. Ebenso könnten Behörden und andere Unternehmen ihre Linux-Strategien damit nicht weiter verfolgen.

Unterstützung für Alt und Neu

Die Schutzsysteme müssen alle eingesetzten Systeme unterstützen, nicht nur die Mehrzahl. Das betrifft zum Beispiel auch die sogenannten Legacy-Systeme, die seit Jahren im Einsatz sind. Beispiel Novell Netware: Trotzdem der Support für die letzte Version im März 2010 eingestellt wurde, setzen viele Unternehmen nach wie vor darauf und brauchen entsprechenden Schutz. Ebenso muss der Schutz so flexibel sein, dass er sämtliche Spielarten der Konfiguration unterstützt, etwa Terminal Server, Cluster, virtuelle Maschinen und bei speziellen Server-Rollen eben auch deren besondere Herausforderungen. Beim Schutz eines Datenbank-Servers ist zum Beispiel wichtig, dass die Schutzsoftware mit hoher Last klarkommt und auch gut skaliert.

Backups anlegen

Regelmäßige Datensicherungen von wichtigen Dateien sind in Unternehmen Pflicht. In vielen Branchen sind sogar Archivierungszeiträume gesetzlich vorgeschrieben, sodass hier noch eine größere Bedeutung für Backups existiert. Aber selbst wenn man keine gesetzlichen Vorgaben hat, sollte man als Unternehmen eine Backup-Strategie entwerfen.

Verwaltung über eine Oberfläche

Das Ziel von Security-Software ist einfach formuliert: Sie soll die Produktivsysteme wirksam vor Bedrohungen schützen. Das gilt im Beispiel von Fileservern für alle Plattformen. Deshalb sollten alle Systeme, egal mit welchem Betriebssystem sie ausgestattet sind, über eine einheitliche Oberfläche verwaltet werden können. So wird auch gezielt die Komplexität für Administratoren reduziert.

Grundschutz weiter ausbauen

Die perfekte Schutzsoftware deckt zum einen die oben dargestellten Grundfunktionen ab, wie ihn alle Unternehmen benötigen. Zum anderen muss die Security-Lösung aber noch deutlich mehr drauf haben, es sind auch Spezialfunktionen gefragt, die optimal auf die darunterliegenden Systeme und die Erfordernisse im Unternehmen zugeschnitten sind. So brauchen Admins eine flexible Möglichkeit um Tasks, etwa gezielte Malware-Scans, zu steuern. So kann man aufwändige Malware-Scans in die Nacht verlagern und hat zu Zeiten der Spitzenlast Performance-Reserven übrig. Apropos Performance:

Eine Schutzlösung für heterogene Systeme muss möglichst gut skalierbar sein, damit sie in einem dynamischen IT-Umfeld nicht zum Flaschenhals wird. Wenn dann unter dem Strich auch das Reporting vereinheitlicht ist, hat man schon fast den perfekten Schutz für sein heterogenes Netzwerk gefunden.

Analyse der IT-Systeme

Doch woher weiß man als Firma, wo man den IT-Grundschutz ausbauen muss? Der erste Schritt auf dem Weg zum Sicherheitskonzept ist eine Analyse der bestehenden IT-Systeme. Das macht man am besten in einem Projektteam. Fangen Sie ruhig allgemein an und zwar am besten mit einer Definition von Funktionen und Aufgaben der Datennetze und Computersysteme. Danach geht man einen Schritt weiter ins Detail und widmet sich den Diensten und Applikationen. Legen Sie auch hier genau die Aufgaben fest und bewerten Sie, wie stark der Geschäftsbetrieb von den einzelnen gefundenen Elementen abhängt. Am Ende sollten Sie eine Prioritätenliste in Händen halten, die klar zeigt, welche IT-Systeme den größten Schutz brauchen und welche weniger wichtig sind.

Schutz für die IT-Umgebung

Das Schutzkonzept muss umfassend sein. Beispielsweise können Sie mit dem Netzwerk anfangen und sich dann zu den Endgeräten vorarbeiten. Die Firewall ist meist das zentrale und offensichtlichste Schutzsystem für Unternehmen. Wichtig ist, dass die eingesetzten Applikationen möglichst automatisch erkannt werden und ohne großen Konfigurationsaufwand funktionieren. Eine moderne Firewall umfasst auch gleichzeitig ein Intrusion Detection und Prevention System. Wichtig: Die Firewall soll aber nicht nur das Firmennetz abschotten. In vielen Firmen gibt es Außendienstler, die von unterwegs auf Mails oder Unternehmens-Software zugreifen müssen. Auch das muss sich möglichst einfach mit der Firewall realisieren lassen. Je nach Einsatzgebiet sollte der Netzwerkzugriffsschutz von Cisco oder Microsoft unterstützt werden. So lässt sich der Netzwerkzugriff für einen PC, abhängig vom aktuellen Sicherheitsstatus, erlauben oder verbieten.

Spezielle Security-Anforderungen für Server

Der Schutz für Clients und Server ist im IT-Grundschutz mit drin. Doch Server ist nicht gleich Server. Je besser eine Security-Komponente auf die Server-Aufgabe

zugeschnitten ist, desto weniger Ressourcen braucht sie. So ist es für Mail-Security sehr wichtig, dass die Nachrichten in Echtzeit gescannt und zuverlässig Phishing-Nachrichten aussortiert werden. Schnelle Ein-Ausgabe-Verarbeitung ist also Pflicht. Beim File-Server müssen sich dagegen gezielt Prozesse vom Virencheck ausschließen lassen, etwa wenn eine Backup-Lösung die Dateien regelmäßig sichert. Wer Cluster, Virtualisierung oder Terminal-Server einsetzt, sollte sich ebenfalls um speziell maßgeschneiderte Security-Komponenten kümmern.

Notfallplan entwickeln

Die passende Sicherheitsstrategie sollte durch einen Notfallplan ergänzt werden. Die nötigen Punkte im Notfallplan entstehen am besten durch eine Risikoanalyse des Unternehmens. In dieser Analyse muss genau geprüft werden, was beim Ausfall welcher Prozesse passieren muss.

Notfallplan testen und Strategie prüfen

Was wäre wenn? Zwar ist es wünschenswert, dass der Notfall nie eintritt, aber Sie sollten es nicht darauf ankommen lassen. Wie eine Feuerwehrübung sollte auch ein IT-Notfallplan alle 6 Monate getestet werden. Ebenso häufig sollten Sie die Sicherheitsstrategie aktualisieren, denn die IT-Anforderungen ändern sich in den meisten Unternehmen sehr schnell.