Handbuch IT-Sicherheit

Eine Handreichung mit Handlungsempfehlungen für Basis-Maßnahmen

DIHK Deutscher Industrie- und Handelskammertag

#GemeinsamSicherHandeln

Inhaltsverzeichnis

Autor:

Datum XXX
Versionskontrolle:

1. Einleitung

Im Dokument „Handbuch IT-Sicherheit" werden Handlungsempfehlungen für die Einrichtung, Aufrechterhaltung und Überprüfung einer angemessenen Informationssicherheit beschrieben. Die hier dargestellten Handlungsempfehlungen beschreiben allgemeine Empfehlungen für IT-Ansprechpartner zu organisatorischen und technischen Maßnahmen. Die Empfehlungen sind dem IT-Grundschutz-Handbuch des BSI entnommen.

2. Empfohlene Sicherheitsmaßnahmen

Der folgende Maßnahmenkatalog trägt dazu bei Informationen abzusichern, indem systematisch notwendige Sicherheitsmaßnahmen identifiziert und umgesetzt werden.

2.1 Systematisches Herangehen an Informationssicherheit

2.1.1 Angemessene Berücksichtigung von Informationssicherheit

Informationssicherheitsaspekte müssen bei allen Projekten frühzeitig berücksichtigt werden

Eine möglichst große Programmvielfalt mit hoher Funktionalität, bequeme Bedienung, niedrige Anschaffungs- und Betriebskosten stehen fast immer in Konkurrenz zur Informationssicherheit. Es empfiehlt sich aber unbedingt, Informationssicherheitsaspekte schon zu Beginn eines Projektes (z. B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) zu berücksichtigen. Gerade neue Techniken dürfen nicht unkritisch eingesetzt werden. Später auftretende Sicherheitsmängel können unangenehme Konsequenzen zur Folge haben. Werden nachträglich Design- oder Planungsfehler offenkundig, sind Nachbesserungen oftmals unverhältnismäßig teuer oder sogar unmöglich. Der Mut, Abstriche beim Komfort zu machen oder auf eine bestimmte Funktionalität zu verzichten, kann hohe Kosten durch Sicherheitsvorfälle verhindern oder hohe Investitionen in zusätzliche Informationssicherheitsprodukte ersparen.

Empfohlene Maßnahmen:
Zu Beginn jedes IT-Projektes sollten Sicherheitsanforderungen erfasst und entsprechend bei der Planung und Umsetzung berücksichtigt werden. Die für die Sicherheitskonzeption und für die Umsetzung der festgelegten Maßnahmen erforderlichen Ressourcen müssen bereits bei der Projektplanung einberechnet werden.

2.1.2 Schritt für Schritt zu mehr Informationssicherheit

Ein Handlungsplan mit klaren Prioritäten der Sicherheitsziele und -maßnahmen sollte erstellt werden

Wer eine Weile über sinnvolle Schritte zur Erhöhung der eigenen Informationssicherheit nachgedacht hat, wird sich bald vor mehr Aufgaben gestellt sehen als er zeitlich und finanziell bewältigen kann. Daher ist eine geeignete Priorisierung identifizierter Sicherheitsziele und -maßnahmen erforderlich.

Empfohlene Maßnahmen:
Es sollten Prioritäten für Sicherheitsmaßnahmen festgelegt und in einem Handlungsplan festgehalten werden. Diese Priorisierung sollte mittels Risikoanalyse und auch unter Abwägung des Kosten-Nutzen-Verhältnisses getroffen werden.

Zuständigkeiten müssen festgelegt werden

Für jede identifizierte Aufgabe muss festgelegt werden, wer für die Durchführung verantwortlich ist. Ebenso sollte für alle allgemein formulierten Sicherheitsrichtlinien genau dargelegt werden, für welchen Personenkreis diese verbindlich sind. Betreffen diese nur die festangestellten Mitarbeiter, eine bestimmte Abteilung oder alle?

Jeder Verantwortliche braucht möglichst einen Stellvertreter. Wichtig ist, dass der Vertreter auch in der Lage ist, seine Aufgaben wahrzunehmen. Wurde er in seine Aufgaben eingewiesen? Sind notwendige Passwörter für den Notfall hinterlegt? Benötigt er Dokumentationen?

Empfohlene Maßnahmen:
Verantwortlichkeiten, inklusive Stellvertreter, sollten für jede sicherheitsrelevante Aufgabe festgelegt und dokumentiert werden.

Richtlinien und Zuständigkeiten müssen bekannt gemacht werden

Es muss sichergestellt sein, dass alle Betroffenen die Nutzungsrichtlinie in ihrer aktuellen Fassung kennen. Alle Mitarbeiter sollten ihre internen und externen Ansprechpartner und deren Kompetenzen kennen. Das dient nicht nur dazu, bei Problemen schneller Hilfe zu erhalten. Es verhindert auch, dass sich Mitarbeiter durch Überredungskunst oder Einschüchterung dazu verleiten lassen, vertrauliche Informationen (Passwörter etc.) an Unberechtigte weiterzugeben.

Hierbei sind auch juristische Aspekte zu berücksichtigen, damit im Falle von Sicherheitsverstößen eine Ahndung nicht bereits daran scheitert, dass sich der Beschuldigte zurecht auf seine Unkenntnis beruft.

Empfohlene Maßnahmen:
Die Richtlinien und organisatorischen Maßnahmen sollten regelmäßig bekannt gemacht werden. Die Zuständigkeiten (z.B. IT-Ansprechpartner) sollten regelmäßig überprüft und bekannt gemacht werden. Auch Veränderungen oder Ergänzungen müssen den Mitarbeitern zeitnah mitgeteilt werden. Im Bedarfsfall ist es vorteilhaft, die Kenntnisnahme wichtiger Richtlinien und organisatorischer Maßnahmen von den Mitarbeitern schriftlich bestätigen zu lassen.

Es dürfen keine Ausnahmen bei den Sicherheitsmaßnahmen gemacht werden

Sicherheitsmaßnahmen dienen dem Schutz der gesamten IT-Umgebung. Dieser Schutz ist allerdings nur so stark wie sein „schwächstes Glied". Daher sollten unbedingt Ausnahmen vermieden werden, die einzelne Nutzer von Sicherheitsmaßnahmen befreien. Dies trifft insbesondere auf Benutzer in leitenden Positionen zu – die Geschäftsleitung inbegriffen.

Empfohlene Maßnahmen:
Sicherheitsrelevante Maßnahmen (wie zum Beispiel lokale Benutzerrechte auf Clientsystemen, Passwortrichtlinien oder Update-Installationen) sollten für alle Anwender gleichermaßen gelten und durchgesetzt werden.

2.1.3 Kontrolle und Aufrechterhaltung der Informationssicherheit

Die Informationssicherheit sollte regelmäßig überprüft werden

Das Niveau der Informationssicherheit sollte regelmäßig kontrolliert und bewertet werden. Die Bewertung sollte anhand des festgestellten Risikos, der Umsetzung der daraus resultierenden Maßnahmen und Best Practice Empfehlungen wie zum Beispiel aktuellen Sicherheitsstandards vorgenommen werden.

Empfohlene Maßnahmen:
Sicherheitsüberprüfungen sollten regelmäßig von unabhängigen Experten durchgeführt werden. Die Erkenntnisse der Überprüfungen müssen dokumentiert und in Form eines geeigneten Reportings an die Geschäftsleitung übergeben werden. Gewonnene Erkenntnisse können wiederum in die Sicherheitskonzeption einfließen. Erkannte Abweichungen beispielsweise bei der technischen Umsetzung von definierten Maßnahmen müssen beseitigt werden.

Am Arbeitsplatz sollte Ordnung herrschen und sensible Informationen sollten nicht frei zugänglich sein

„Ordnung ist das halbe Leben". Über diesen Spruch mag man geteilter Meinung sein. Im Zusammenhang mit Informationssicherheit ist Ordnung zweifelsfrei ein hervorragendes Mittel zur Vermeidung zahlreicher Risiken.

Empfohlene Maßnahmen:
Vertrauliche Akten sollten bei Verlassen des Arbeitsplatzes im Schrank oder Safe verschlossen werden. Datenträger wie Bänder, USB-Sticks, externe Festplatten, BDs, DVDs oder CDs sollten nie offen herumliegen, wenn sich vertrauliches Material darauf befindet. Im Bedarfsfall sollten sie sachgerecht vernichtet und entsorgt werden, um unbefugtes Rekonstruieren zu verhindern. Auch vertrauliche Ausdrucke gehören zur Entsorgung in den Aktenvernichter und nicht in den normalen Papierkorb.

Erkannte Sicherheitsverstöße sollten auch sanktioniert werden

Es sollte allen Beteiligten bewusst sein, dass die (absichtliche oder versehentliche) Missachtung von Sicherheitsvorgaben Konsequenzen nach sich zieht. Um diesen Sachverhalt zu unterstreichen, sollte jeweils klar vermerkt werden (beispielsweise in der organisationseigenen Sicherheitsrichtlinie), mit welchen Folgen im Ernstfall zu rechnen ist.

Werden Sicherheitsverstöße aufgedeckt, so stellt sich unmittelbar die Frage, wie Vorgesetzte dem Verursacher gegenüber auftreten sollen.

Harte Sanktionen bei leichten Verstößen sind sicherlich unangemessen, besonders falls es sich um das erste Mal handeln sollte. Ebenso falsch ist es jedoch, bei schwereren Verstößen oder hartnäckigen Verweigerern auf Sanktionierung zu verzichten. Dies setzt nicht nur beim Verursacher falsche Signale, sondern auch bei allen anderen, die davon erfahren. Daher muss im Bedarfsfall angemessen reagiert werden. Die Tatsache, dass Verstöße geahndet werden, muss allen anderen kommuniziert werden, soweit die jeweilige Situation dies erlaubt.

Empfohlene Maßnahmen:
Zu jeder Sicherheitsrichtlinie sollten bestimmte Konsequenzen oder Sanktionen zugeordnet sein. Diese Regelung sollte allen Mitarbeitern bekannt gemacht – und umgesetzt – werden. Sobald ein Sicherheitsverstoß erkannt wird, sollten angemessene Konsequenzen bzw. Sanktionen erfolgen. Diese sollten in einem passenden Verhältnis zum tatsächlichen Schweregrad des Vergehens stehen

2.2 Sicherheit von IT-Systemen

Im Folgenden werden typische Anforderungen und zugehörige Maßnahmen beschrieben.

Supportverträge für Hard- und Software müssen regelmäßig vor Ablauf aktualisiert werden

Server-Hardware oder andere wichtige zentrale Komponenten sollten sich noch innerhalb der Frist für den Hersteller-Support befinden. Nur so kann sichergestellt werden, dass bei einem defekten Bauteil oder einem Komplettausfall kurzfristig Abhilfe geschaffen und die Verfügbarkeit gewährleistet werden kann. Zeitlich befriste Verträge müssen ebenfalls regelmäßig verlängert werden.
Auch bei anderen Komponenten (wie zum Beispiel Virenschutz oder Firewalls) sind die Updates an zeitlich befristete Lizenz- oder Supportverträge (Abo) geknüpft. Läuft die entsprechende Nutzungslizenz oder der Supportvertrag aus, können keine weiteren Aktualisierungen eingespielt werden oder einige Funktionen stehen nicht mehr zur Verfügung. In solchen Fällen ist also darauf zu achten, Lizenz- oder Supportverträge rechtzeitig vor deren Ablauf zu verlängern, um weiterhin kontinuierlich mit Updates versorgt zu werden. Ist dies nicht möglich, ist eine Außerbetriebnahme rechtzeitig zu planen.

Empfohlene Maßnahmen:
Alle Komponenten sollten mit Informationen bezüglich der Laufzeit von Lizenz- oder Supportverträgen in einer zentralen Liste erfasst und regelmäßig kontrolliert werden. Auslaufende Verträge sollten rechtzeitig verlängert werden. Sollte eine Verlängerung aufgrund des Alters der Komponenten nicht mehr möglich sein, sollte diese ebenfalls rechtzeitig durch neue ersetzt werden, um so längere Ausfallzeiten vorbeugend zu verhindern.

Rechtzeitige Aktualisierung von Zertifikaten erforderlich

Auch abgelaufene öffentliche oder interne Zertifikate können einen Ausfall oder eine Störung von Diensten verursachen.

Empfohlene Maßnahmen:
Die Ablaufdaten der eingesetzten Zertifikate sollten ebenfalls in einer Liste erfasst werden. Die Zertifikate sollten rechtzeitig vor deren Ablauf erneuert werden.

Virenschutzprogramme müssen flächendeckend eingesetzt werden

Ein stets aktueller flächendeckender Virenschutz ist unverzichtbar. Schadprogramme können über Datenträger oder über Netze (Internet, Intranet) in die eigene Umgebung gelangen und verbreitet werden. Selbst für Rechner ohne Internetanschluss sind daher solche Schutzprogramme Pflicht!

Empfohlene Maßnahmen:
Jeder Server und Client sollte mit einem lokalen Virenschutzprogramm ausgestattet sein, das ständig im Hintergrund läuft und regelmäßig mit neusten Updates und Virensignaturen versorgt wird. In der Regel genügt es, nur ausführbare Dateien, Skripte, Makrodateien etc. in Echtzeit zu überprüfen. Ein vollständiges Durchsuchen aller Dateien empfiehlt sich trotzdem in regelmäßigen Abständen (z. B. vor einer Wochensicherung oder während der Sicherung durch eine zusätzliche Virenschutzfunktion der Backup-Lösung). Im Falle eines Schadprogrammbefalls sollte dies in jedem Fall erfolgen.

Die ausgewählte Virenschutzlösung sollte über eine zentrale Verwaltungsmöglichkeit verfügen. Diese ermöglicht in der Regel eine zentrale Konfiguration der Virenschutzsoftware, die Erfassung vorhandener Server und Clients, die Verteilung bzw. Installation sowie die Aktualisierung der Virenschutzsoftware, eine Steuerung von Suchvorgängen und eine Erfassung von Statusinformationen wie Malware-Befall oder Aktualität der Signaturen. Diese Statusinformationen sollten in Form von Berichten einen guten Überblick über den Zustand des unternehmensweiten Virenschutzes liefern, die beispielsweise regelmäßig vom IT-Ansprechpartner oder auch von der Geschäftsleitung geprüft werden. Im Idealfall sollte über zentrale Verwaltung auch eine automatische Benachrichtigung per E-Mail an verantwortliche Mitarbeiter über gefundene Malware konfigurierbar sein.

Zusätzlich empfiehlt es sich, E-Mails und jegliche Kommunikation über das Internet zentral beispielsweise auf der Firewall auf Malware zu untersuchen.

Im Zusammenhang mit festgestellter Schadsoftware ist in jedem Fall der IT-Notfall-Prozess durchzuführen.

Allen Benutzern sollten Rollen und Profile zugeordnet werden

Eine der goldenen Regeln der Informationssicherheit ist das „Need-To-Know-Prinzip": Jeder Benutzer (und auch jeder Administrator) sollte nur auf die Datenbestände zugreifen und die Programme ausführen dürfen, die er für seine tägliche Arbeit auch wirklich benötigt. Dazu gehört auch, dass Informationen einer Abteilung (z. B. Vertrieb, Entwicklung, Personal, Leitung etc.) nicht ohne weiteres von abteilungsfremden Mitarbeitern einsehbar sind, sofern sie diese Informationen nicht für ihre Arbeit benötigen. Anwendungsprogramme – insbesondere Programme für die Systemadministration – sollten ebenfalls nur den Mitarbeitern zur Verfügung stehen, die diese wirklich brauchen.

Empfohlene Maßnahmen:
Die Umsetzung dieses Prinzips ist mit vertretbarem Aufwand möglich. Erforderliche Berechtigungen und Rechte werden in passenden Berechtigungsprofilen zusammengefasst. Auf deren Grundlage werden dann wahlweise geeignete Benutzergruppen oder Rollen definiert. Die individuellen Berechtigungen und Rechte eines Systembenutzers lassen sich über dessen Gruppenzugehörigkeiten oder über die Rollen steuern, die der Benutzer annehmen darf.
Die Nutzung von Berechtigungsgruppen bei der Zuweisung von Berechtigungen gilt auch für andere zentrale Ressourcen. Beispielsweise sind das Freigaben, Öffentliche Ordner im Exchange, Datenbanken oder einzelne Bereiche im Intranet. Die Namenskonventionen für Berechtigungsgruppen sollten ebenfalls im Berechtigungskonzept fixiert werden. So muss später nicht jede einzelne vergebene Berechtigung dokumentiert werden, sondern aus dem Namen einer Gruppe ist erkennbar, welche Ressourcen mit welcher Berechtigung zugewiesen sind.

allgemein	Typ_Ziel_Berechtigung	Typ Ressourcentyp Ordnername Zielordner Berechtigung Berechtigungskürzel
Ordner Personal	fs_personal_fc	Mitglieder haben Vollzugriff auf den Ordner Personal und in der Regel auf alle darunter befindlichen Objekte im Fileservice
Ordner Personal	fs_personal_c	Mitglieder haben Änderungsrechte auf den Ordner Personal und in der Regel auf alle darunter befindlichen Objekte im Fileservice
Ordner Personal	fs_personal_r	Mitglieder haben Leserechte auf den Ordner Personal und in der Regel auf alle darunter befindlichen Objekte im Fileservice

Tabelle 1 – Beispiel Namenskonventionen für Berechtigungsgruppen

In regelmäßigen Abständen sollte überprüft werden, ob die von einer Person verfügbaren Zugriffsrechte noch deren Tätigkeitsprofil entsprechen oder ob Änderungen wie Einschränkungen oder Erweiterungen zweckmäßig wären.
Um einen Überblick über vorhandene Zugriffsberechtigungen zu erhalten, sollten eigene Systeme regelmäßig mit Stichproben oder passenden Tools untersucht werden.
Ebenso muss ein geeigneter Prozess existieren, um Berechtigungen bei Einstellung, Funktionsänderung oder Weggang von Mitarbeitern geeignet einzuräumen bzw. zu widerrufen.

Ein Lebenszyklus für Benutzerkonten sollte definiert sein

Benutzerkonten von ausgeschiedenen Mitarbeitern sind weiterhin mit zugeordneten Rollen aktiv und es besteht die Gefahr eines unbemerkten Missbrauchs.

Empfohlene Maßnahmen:
Wie der Mitarbeiter selbst unterliegt auch sein Benutzerkonto (teilweise auch mehrere) einem Lebenszyklus. Das beginnt mit der Erstellung. Danach erfolgt die Pflege beispielsweise bei Rollenwechseln. Bei Ausscheiden des Mitarbeiters sollte das Konto zunächst sofort deaktiviert und nach einer kurzen Karenzzeit (zwei Monate) gelöscht werden. Der administrative Umgang mit Benutzerkonten (auch Gruppenkonten) sollte in einem Lebenszyklus definiert werden.

Administratorrechte sollten auf das erforderliche Maß eingeschränkt werden

Viele Systemadministratoren arbeiten unter einer administrativen Rolle, die praktisch keinen Einschränkungen unterliegt und alle Systemprivilegien beinhaltet. Dies ermöglicht zum einen den Missbrauch durch den Administrator selbst, andererseits erhöht sich das Risiko im Falle einer erfolgreichen Übernahme der Administrator-Rolle durch unbefugte Dritte. Daher sollte nach Möglichkeit zwischen unterschiedlichen administrativen Aufgaben differenziert werden. Je nach administrativer Rolle kann beispielsweise ein Administrator bestimmte Dienste verwalten, ein anderer kann neue Benutzer anlegen oder Kennwörter zurücksetzen, ein Dritter ist für Backups zuständig. Im Idealfall gibt es sogar einen gesonderten Administrator, der die Auswertung von Protokollierungsdaten vornimmt und die Aufgaben der anderen Administratoren überwachen kann.

Empfohlene Maßnahmen:
Notwendige administrative Rechte sollten überprüft und gegebenenfalls beschränkt werden. Beispielsweise benötigen Dienstleister nur administrative Rechte auf einem bestimmten System für die Betreuung eines bestimmten Dienstes aber keine administrativen Rechte in der gesamten Umgebung.

Programmprivilegien sollten begrenzt werden

Programme verfügen bei ihrer Ausführung über bestimmte Zugriffsrechte und Systemprivilegien. In vielen Fällen erbt ein Programm einfach die Berechtigungen des Benutzers, der es gestartet hat. Manchmal genügen diese Berechtigungen nicht oder es handelt sich um Serverprozesse, die oft mit hohen Privilegien ausgestattet sein müssen. In solchen Fällen besitzen Programme manchmal administrative Rechte und können ebenso wie ein „allmächtiger" Systemadministrator alle Systemressourcen nutzen. Werden solche Programme von einem Angreifer zweckentfremdet, so erbt dieser wiederum alle Rechte des missbrauchten Programms. Aus diesem Grunde dürfen auch Programme nur mit den Berechtigungen ausgestattet sein, die sie für ein fehlerfreies Funktionieren benötigen.

Empfohlene Maßnahmen:
Für bestimmte Dienste (Services) und geplante Aufgaben (Scheduled Tasks) sollten spezielle, nur für diese jeweilige Funktion verwendete Benutzerkonten – sogenannte Dienstkonten – angelegt werden. Diese erhalten dann ausschließlich die minimalen Berechtigungen, die für die entsprechende Funktionalität benötigt werden. Auf den Gebrauch von administrativen Konten (in jedem Fall Domänen-Administratoren) sollte verzichtet werden. Auch die Verwendung von administrativen Konten von Mitarbeitern sollte unterbleiben, da in einem solchen Fall die Änderung von Passwörtern zu Ausfällen führt. Dabei gilt: Für jeden Dienst, für jedes System sollte ein spezielles Konto erstellt werden, um so eine Änderung von Passwörtern möglich zu machen oder das Konto bei Außerbetriebnahme zu löschen.

Die Standardeinstellungen gemäß Auslieferungszustand sollten angepasst werden

Viele Betriebssysteme und Software-Applikationen sind vom Hersteller (oder von Dienstleistern) derart vorkonfiguriert, dass nach erfolgter Installation ein möglichst reibungsloser und komfortabler Betrieb ermöglicht wird. Die gleiche Aussage gilt für andere IT-Systeme (Firewalls, WLAN Access Points, Switches) und TK-Anlagen. Informationssicherheitsaspekte spielen leider häufig keine Rolle bei der Wahl der Standardinstallation durch den Hersteller. Zweifelsohne ist dieser Komfort für all jene Benutzer angenehm, die mit dem betreffenden System nicht oder noch nicht hinreichend vertraut sind. Die vorhandene Produktfunktionalität wird in der Grundkonfiguration möglichst wenig eingeschränkt und erlaubt die ungestörte Kommunikation mit der eigenen Umgebung. Häufig sind Standard-Passwörter und Standard-Benutzer-Accounts eingerichtet. Um Missbrauch zu vermeiden, müssen diese deaktiviert werden.

Ein frisch installiertes und noch nicht an die eigenen (Sicherheits-) Bedürfnisse angepasstes System sollte deshalb nie im produktiven Betrieb genutzt werden!

Empfohlene Maßnahmen:
Standardbenutzer und Passwörter sollten geändert oder deaktiviert und durch individuelle Benutzerkonten ersetzt werden. Dies betrifft beispielsweise Firewalls, Switches, WLAN Access Points und TK-Anlagen.

Betriebssysteme besonders exponierter Rechner sowie wichtige Server müssen gehärtet werden. „Härten" (engl. Hardening) bedeutet in der Informationssicherheit die Entfernung aller Softwarebestandteile (Rollen und Funktionen), die zur Erfüllung der vorgesehenen Aufgabe nicht zwingend notwendig sind. Oftmals gelingt einem Angreifer der Einbruch in einen Server durch den Missbrauch eines Programms, das auf diesem Server gar nicht installiert sein müsste. Außerdem macht die regelmäßige Pflege und Aktualisierung eines Rechners natürlich mehr Arbeit, wenn dieser mehr Programme enthält. Aus diesen Gründen sollten auch alle unnötigen Anwendungsprogramme (Adobe Reader, unnötige Webbrowser, Tools zum Entpacken etc.) gar nicht installiert oder umgehend entfernt werden.

Auch eine permanente Verbindung ins Internet ist bei einigen Servern entbehrlich.

Installations- und Konfigurationsdokumentationen müssen erstellt und regelmäßig aktualisiert werden

Eine Dokumentation von Systemen und anderen Komponenten (Installation und Konfiguration) ist notwendig, um im Problemfall, insbesondere auch bei Sicherheitsvorfällen entstandene Abweichungen durch Manipulation zu erkennen, die möglichen Ursachen aufzufinden und zu beseitigen oder einen definierten Zustand wiederherzustellen. Eine Dokumentation ist somit auch für den Notfall oder bei der Wiederherstellung und dem Wiederanlauf im Normalbetrieb unerlässlich.

Es ist wichtig, dass die Dokumentation auch von Dritten (beispielsweise im Sinne eines „Ersatz-Administrators" oder einer Urlaubsvertretung) nachvollzogen und verstanden werden kann. Dadurch werden Ausfallrisiken reduziert, wenn der hauptamtliche Administrator oder Dienstleister plötzlich nicht mehr zur Verfügung stehen sollte.

Eine Installations- und Konfigurationsdokumentation kann auch die Standardisierung im Sinne von Vorgaben bei einer möglichen Wiederholung der Bereitstellung (Clientsysteme) unterstützen.

Empfohlene Maßnahmen:
Alle Arbeitsschritte während einer Installation und Konfiguration sowie nachträgliche Änderungen (Abweichungen und Ausnahmen) sollten schriftlich dokumentiert werden. Die Dokumentation sollte im Wesentlichen möglichst „schlank" gehalten und nur Abweichungen gegenüber den Herstellerstandards enthalten, um so den Aufwand zu minimieren und die Nachvollziehbarkeit zu gewährleisten. Änderungen und Ausnahmen können auch in einer Art Logbuch oder, falls vorhanden, in einem Ticketsystem festgehalten werden. Werden die Systeme durch einen IT-Dienstleister betreut bzw. bereit gestellt, ist die Dokumentation vom IT-Dienstleister einzufordern.

Es sollten nur notwendige Systeme betrieben werden

Bei der Einführung neuer Komponenten sind in einer Übergangsphase alte vorhandene und neue Systeme im Betrieb. Mitunter besteht kein definierter Zustand, der eine Wartung oder im Notfall eine entsprechende Wiederherstellung ermöglicht.

Auch die Konsolidierung verschiedener Systeme kann eine Verbesserung mit sich bringen, da jedes aus der IT-Landschaft entfernte System eine Verringerung des Gefahrenpotentials, des Wartungsaufwands und nicht zuletzt der Angriffsfläche des Unternehmens bedeutet.

Empfohlene Maßnahmen:
Altsysteme sollten zeitnah nach dem Auslaufen des Supports außer Betrieb genommen werden. Die Außerbetriebnahme von Altsystemen sollte bei der Einführung neuer Systeme geplant und systematisch durchgeführt werden. Die Übergangsphase sollte möglichst kurz gehalten werden. Es sollte auch regelmäßig überprüft werden, welche Server, Testsysteme oder andere Komponenten nicht mehr benötigt werden. Diese sollten außer Betrieb genommen und aus der Umgebung entfernt werden.

Auch eine Konsolidierung einzelner Systeme kann den Wartungsaufwand sowie die potenzielle Angriffsfläche verringern.

Mobile Geräte erfordern besondere Sicherheitsmaßnahmen

Häufig werden neben herkömmlichen Arbeitsplatzrechnern auch Notebooks, Tablets oder Smartphones für den Zugriff auf Daten (z.B. Dokumente, Kontaktdaten) oder andere interne Ressourcen (z.B. E-Mail-Dienste) verwendet. Da sich diese „mobilen Geräte" aus unterschiedlichsten Netzen heraus mit der IT-Umgebung des Unternehmens verbinden und zusätzlich auch viel stärker den Gefahren von Diebstahl oder Manipulation ausgesetzt sind, gilt es hierbei eine Reihe von besonderen Sicherheitsmaßnahmen zu berücksichtigen.

Empfohlene Maßnahmen:
Für Notebooks sollte eine Vollverschlüsselung der Festplatte (z. B. per Microsoft BitLocker oder Apple FileVault) erfolgen. Die Personal-Firewall sollte aktiviert werden und der Virenschutz und Softwarestand aktuell sein. Die Verwendung von lokalen administrativen Rechten sollte nur in Ausnahmen erfolgen und zusätzlich durch die Benutzerkontensteuerung (auf aktuellen Windows-Systemen) geschützt werden. Siehe dazu auch die Sicherheitsmaßnahmen „Vorhandene Schutzmechanismen nutzen" und „Sensible Daten".

Für Smartphones und Tablets sollten Richtlinien und Maßnahmen definiert und organisatorisch durch eine Nutzungsrichtlinie vorgeschrieben oder technisch erzwungen werden, die eine Absicherung des Gerätes per Passwort bzw. PIN (komplex und zyklischer Wechsel) voraussetzen. Zudem sollte – falls vom jeweiligen Endgerät unterstützt – eine Verschlüsselung des Geräts bzw. dessen Speichers vorgeschrieben werden.

Smartphones und Tablets sollten möglichst in einer Mobile Device Management Lösung (MDM, beispielsweise per Microsoft Exchange) verwaltet oder mindestens herstellerseitig (z.B. Apple „iPhone-Suche") erfasst werden. Dadurch kann bei Diebstahl oder Verlust das entsprechende Gerät per „Remote Wipe"aus der Ferne gelöscht werden, um so den unbefugten Zugriff auf sensible Daten zu verhindern, die auf dem Gerät enthalten sind.

Der Zugriff mit Smartphones und Tablets auf E-Mails, Kontakte und Termine sollte über Push-Verfahren (beispielsweise ActiveSync) erfolgen. Dafür sollte eine selektive und keine generelle Freischaltung erfolgen. Die dafür erforderliche Veröffentlichung der vorhandenen Groupware (Microsoft Exchange, Lotus Notes usw.) ins Internet sollte dabei optional über Reverse Proxys innerhalb einer Demilitarisierten Zone, einer Zwischenzone zwischen Intranet und Internet, gelöst werden. Dies erschwert den unerlaubten Zugriff auf diese Ressourcen und dient als zusätzliche Barriere, an der auch weitere Sicherheitsprüfungen des Datenverkehrs aus dem Internet erfolgen können, die durch die Groupware selbst nicht angeboten werden können.

Analog zu den Vorgaben zu Hard- und Software sollte auch die Firmware der mobilen Geräte regelmäßig auf den neuesten Update-Sstand gebracht werden. Jailbreaks und Device-Rooting dürfen auf keinen Fall zugelassen werden, da sie die Sicherheit des Endgerätes gefährden.

Notebooks und andere mobile Geräte oder auch Datenträger sollten nie unbeaufsichtigt im Auto zurückgelassen werden und sind ggf. auch im Büro – nachts oder bei längerer Abwesenheit – einzuschließen.

2.3 Vernetzung und Internetanbindung

Zum Schutz von internen Netzen muss eine Firewall verwendet werden

Kein Computer, der geschäftsmäßig genutzt wird, darf ohne Schutz durch eine geeignete Firewall mit dem Internet verbunden werden. Dies betrifft gleichermaßen Server- und Clientsysteme.

Auch innerhalb größerer interner Netze existieren normalerweise mehrere Teilnetze mit unterschiedlichen Benutzergruppen und unterschiedlichem Schutzbedarf. Das „eigene" Teilnetz muss daher oftmals gegen benachbarte Netze abgesichert werden, um Bedrohungen vorzubeugen, die qualitativ mit jenen aus dem Internet vergleichbar sind (z. B. Abschottung der Personalabteilung gegen den Rest des Unternehmens [oder Abschottung des Unternehmensnetzwerks gegen ein Gäste-WLAN]). In diesem Fall sollten auch an diesen Netzübergängen Schutzmechanismen installiert werden.

Empfohlene Maßnahmen:
Die Verbindung zwischen dem internen Netzwerk und dem Internet – oder auch anderen Netzen – muss durch eine Firewall abgesichert werden. Ein entsprechendes Hard- oder Softwaresystem muss implementiert werden.

Generell empfiehlt es sich alle Server- und Clientsysteme bei Verfügbarkeit einer Personal Firewall (Bestandteil von Windows Betriebssystemen) zusätzlich abzusichern. Einzelne Systeme wie Notebooks mit Zugang zu öffentlichen Netzen (WLAN-Hotspots) und nicht kontrollierten Netzen (bei Kunden) müssen zusätzlich mit einer Personal Firewall abgesichert werden.

Eine sichere Firewall muss regelmäßig überprüft werden

Zum Schutz des internen Netzes gegen benachbarte, weniger vertrauenswürdige Netze muss ein geeigneter Firewall-Typ ausgewählt werden. Die Konzeption der Firewall-Architektur und die Installation und Konfiguration der Firewall sollte Spezialisten vorbehalten bleiben. In der Regel empfiehlt sich ein mehrstufiges Firewall-Konzept, bei dem zusätzliche Filterelemente vor- und nachgeschaltet werden.

Die Filterregeln in Firewalls neigen dazu, im Laufe der Zeit länger und unübersichtlicher zu werden. Firewall-Administratoren geben nachträglichen Anforderungen der Anwender oft allzu leicht nach und weichen die Regeln auf. Auch für die Geschäftsleitung sollten keine Ausnahmen gemacht werden!

Empfohlene Maßnahmen:
Eine Firewall-Konzeption muss erstellt werden. Anhand dieser Konzeption muss eine geeignete Firewall-Lösung implementiert und durch eine entsprechende Konfiguration (Regelwerk) gemäß fixierten Anforderungen angepasst werden. Wobei eine restriktive Herangehensweise mit nur den tatsächlich benötigten Portfreigaben mit möglichst eingeschränkten Quellen und Zielen gewählt werden sollte. Bei der temporären Einrichtung zusätzlicher Portfreigaben müssen diese nach Gebrauch wieder entfernt werden, um keine unnötigen Angriffsmöglichkeiten zu bieten. Es muss regelmäßig geprüft werden, ob die bestehenden Filterregeln noch konsistent sind, ob sie vereinfacht werden können und ob sie noch hinreichend restriktiv sind. Gemäß den gewonnenen Erkenntnissen sollte das Regelwerk demnach regelmäßig gegebenenfalls angepasst werden. Sämtliche Einstellungen und Freigaben auf der Firewall müssen in einer detaillierten Dokumentation festgehalten werden, die auch bei Änderungen (auch temporären) entsprechend angepasst werden muss.

Außerdem sollte von Zeit zu Zeit überprüft werden, ob die bestehende Firewall-Konzeption noch den bereits eingeführten oder in Kürze zu erwartenden Kommunikationsprotokollen aus Sicht der Informationssicherheit gewachsen ist. Ebenso können neue Techniken zusätzliche Herausforderungen an bestehende Firewall-Lösungen stellen oder deren Ablösung notwendig machen.

Für mögliche Untersuchungen von Sicherheitsvorfällen sollte sämtlicher Netzwerkverkehr auf der Firewall protokolliert werden. Optional sollte eine automatische Benachrichtigung per E-Mail an Verantwortliche bei Eintreffen vordefinierter Ereignisse oder einem Erreichen von Schwellwerten konfiguriert werden.

Die Firmware der Firewall oder die eingesetzte Software sollten periodisch hinsichtlich verfügbarer Updates und Patches überprüft und aktualisiert werden, da hierbei eigene Sicherheitslücken geschlossen oder hilfreiche zusätzliche Funktionen integriert werden.

Für eine erhöhte Sicherheit werden Firewall-Lösungen mit integrierten Technologien wie z. B. „Virtual Private Network" (VPN, Standortkopplung und gesicherte Verbindung für Mitarbeiter und Dienstleister von außen), „Intrusion Detection System" (IDS, erkennt unerlaubtes Eindringen) oder „Unified Threat Management" (UTM, Scannen des eingehenden Verkehrs auf Schadsoftware) empfohlen. Da UTM Schadsoftware auf der Basis von Signaturen erkennt, müssen diese regelmäßig (mindestens täglich) aktualisiert werden.

Es empfiehlt sich, einen Dienstleister mit der Einrichtung und Pflege der Firewall zu betrauen. Dieser sollte idealerweise entsprechende Zertifizierungen vorweisen können.

Nach außen angebotene Informationen, Dienste und Programmfunktionalität sollten auf das erforderliche Mindestmaß beschränkt werden

Alle Informationen, Funktionen, Serverdienste und offenen Kommunikations-Ports, die nach außen angeboten werden, erhöhen das Risiko einer möglichen Sicherheitslücke. Deshalb sollte in jedem einzelnen Fall sorgfältig geprüft werden, ob es wirklich erforderlich ist, einen potenztiellen „Problemkandidaten" zu aktivieren und nach außen anzubieten. Das damit verbundene Sicherheitsrisiko kann in Abhängigkeit von der jeweiligen Technik und Implementierung sehr unterschiedlich sein.

Empfohlene Maßnahmen:
Bei bestehenden Installationen sollte regelmäßig überprüft werden, ob einzelne Dienste oder Funktionen nicht schlicht aus Versehen oder Bequemlichkeit aktiviert sind, obwohl sie von niemandem benötigt werden.

All jene Server, die aufgrund ihrer Funktionalität eine direkte Kommunikation mit dem Internet erfordern und von diesem nur noch durch Firewalls oder andere Schutzmechanismen (z. B. Proxys) getrennt sind, sollten in einer so genannten „Demilitarisierten Zone" (DMZ) positioniert werden. Hier spielt die richtige Kaskadierung und Untergliederung der Server in verschiedene Teilbereiche der DMZ (mit jeweils eigenen IP-Adressbereichen) eine wesentliche Rolle für die Gesamtsicherheit.

Aus dem Internet erreichbare Server sollten zudem durch Härtung und Konfigurationsanpassung (siehe Sicherheitsmaßnahme zu „Standardeinstellungen") abgesichert werden. Zusätzlich können regelmäßige Auswertungen der System- und Zugriffsprotokolle Aufschluss über eventuell erfolgte Angriffe geben. Die Web-Server sollten möglichst in einer DMZ betrieben werden.

Externe Zugänge müssen abgesichert werden

Es kann vorkommen, dass Mitarbeiter von anderen Standorten, von unterwegs oder vom Heimarbeitsplatz auf interne Ressourcen zugreifen wollen. Häufig müssen auch externe Dienstleister von außen auf interne Systeme zugreifen z. B. in Supportfällen oder für Wartungsarbeiten. Hierbei sind mehrere Sicherheitsaspekte zu beachten.

Empfohlene Maßnahmen:
Es sollte dringend darauf verzichtet werden, einzelne Server per Remote Desktop Protocol (RDP) oder ähnlichen Protokollen (VNC) im Internet zu veröffentlichen, um einen direkten externen Zugriff zu ermöglichen. Besonders ohne weitere Einschränkungen des Zugriffs, beispielsweise anhand erlaubter IP-Adressbereiche, bietet sich hier eine große Angriffsfläche. Ein derartiger externer Zugriff muss über eine gesicherte verschlüsselte Verbindung (VPN) auf ein bestimmtes Gerät (beispielsweise Firewall) erfolgen, von welchem dann weitere Verbindungen auf andere Server per RDP oder ähnliche Protokolle möglich sind. Im Falle einer Veröffentlichung eines internen RDP-Servers (beispielsweise für Mitarbeiter anderer Standorte) kann auch alternativ zu einer VPN-Lösung in der DMZ ein sogenannter RD Gateway (verfügbar ab Windows Server 2008) für die Pre-Authentifizierung und Weiterleitung der Zugriffe eingeführt werden.

Dienstleister sollten dabei für alle administrativen Eingriffe ebenfalls personalisierte Benutzerkonten verwenden. Diese können bei Bedarf aktiviert oder deaktiviert werden. Dadurch lassen sich die externen Zugriffe (in Verbindung mit der Protokollierung) und die vorgenommenen Änderungen jeweils einer bestimmten Person zuordnen, was die Transparenz und Nachvollziehbarkeit erhöht und willkürlichen Zugriffen vorbeugt.

Netzwerkfreigaben sollten restriktive Berechtigungen besitzen

Innerhalb eines Netzwerks aus Servern und Clients ist häufig die zentrale Bereitstellung von Dateien und anderen Informationen ein wichtiger Aspekt für produktive Zusammenarbeit. Auf Servern können hier über freigegebene Ordner Dateien auf unterschiedliche Art und Weise zur Verfügung gestellt werden. Über hinterlegte Berechtigungen werden Benutzer autorisiert, Elemente zu lesen, zu erstellen, zu bearbeiten, zu löschen oder auch deren Berechtigungen zu ändern.

Hierbei sollte beachtet werden, dass die Pflege und Anpassung von Berechtigungen sehr arbeitsintensiv sein können, wenn diese direkt einzelnen Benutzerkonten zugewiesen werden. Falls hier keine sorgfältige Dokumentation der Berechtigungen erfolgt, ist die Nachvollziehbarkeit kaum gegeben und der Aufwand bei eventuellen Anpassungen sehr hoch.

Empfohlene Maßnahmen:
Anstelle von einzelnen Benutzern sollten für fast alle freigegebenen Ordner bzw. für bestimmte Zweige in der Ordnerstruktur separate individuelle Berechtigungsgruppen gemäß Namenskonzept verwendet werden. Diesen Berechtigungsgruppen werden dann berechtigte Benutzer als Mitglieder zugewiesen oder auch bei Ausscheiden oder Rollenwechsel wieder entfernt. Für eine bessere Nachvollziehbarkeit sollten für die Vergabe von Freigabeberechtigungen auf Windows Server-Systemen die Standardgruppe „Authenticated Users" mit Vollzugriff und für die Vergabe von granularen NTFS-Berechtigungen individuelle Domänengruppen verwendet werden. In Ausnahmefällen (persönliche Datenverzeichnisse) können NTFS-Berechtigungen einzelnen Benutzern zugewiesen werden.

WLAN und Netzwerkanschlüsse müssen angemessen abgesichert sein

Durch die zunehmende Verbreitung mobiler Geräte wie zum Beispiel Notebooks, Tablets und Smartphones am Arbeitsplatz hat auch WLAN eine größere Bedeutung erlangt und bedarf daher entsprechender Aufmerksamkeit bzw. Absicherung.

Besprechungsräume werden oft untervermietet oder unterliegen nicht der permanenten Aufsicht durch Mitarbeiter bei der Anwesenheit von Gästen. Vorhandene Netzwerkanschlüsse sind dennoch oft permanent mit dem internen Netzwerk verbunden.

Um Gästen, die Zugang zum Internet benötigen, nicht Zugriff auf interne Systeme oder Daten gewähren zu müssen, hat sich die Einrichtung zweier separater WLAN-Netze bewährt.

Empfohlene Maßnahmen:
Netzwerkanschlüsse in Besprechungsräumen sollten im Normalfall nicht verbunden – also physikalisch an das Netzwerk angeschlossen – sein, sondern nur bei Bedarf bzw. auf Anfrage temporär beschaltet werden. Für Gäste, z. B. im Fall einer Untervermietung der Besprechungsräume, kann ein Zugang in das Gästenetz geschaltet werden, das analog zum Gäste-WLAN nur einen reinen Internetzugang bietet.

Das interne WLAN ist nur für Mitarbeiter vorgesehen und verfügt über eine Anbindung an das firmeninterne Netzwerk. Das Gäste-WLAN hingegen sollte lediglich einen Internetzugang bereitstellen, nicht jedoch einen Zugriff auf interne Ressourcen ermöglichen. Mindestens sollten diese beiden Netze durch eine Firewall oder idealerweise auch physikalisch voneinander getrennt werden, um nicht bei etwaigen Fehlkonfigurationen in den Access Points versehentlich eine Verbindung beider Netze zu schaffen.

Für die Authentifizierung im internen WLAN sollte ein RADIUS-Server anhand der persönlichen Benutzerkonten (WPA2 „Personal") eingesetzt werden. Das Gäste-WLAN muss mindestens über einen Zugriffsschlüssel gesichert werden. Alternativ können mit der Verwendung eines WLAN-Controllers sogenannte „WLAN-Tickets" ausgestellt werden, die einen befristeten Zugang zum Gäste-WLAN ermöglichen. Sollte für beide oder nur ein WLAN für den Zugang verwendet werden, sollte der Zugriffsschlüssel eine Länge von 20 Zeichen besitzen und regelmäßig geändert werden.

Auf Maßnahmen, die keinen wirklichen Zugewinn an Sicherheit bieten, sollte verzichtet werden. Hier wären beispielsweise das Verstecken des WLAN-Namens (SSID) oder eine Filterung per Hardware-ID (MAC-Adresse) zu nennen. Diese können einerseits leicht umgangen werden, erschweren zugleich aber legitimen Benutzern den Zugang zum WLAN.

Als Verschlüsselungstechnologie sollte in kabellosen Netzwerken stets WPA2 verwendet werden. Auf den Einsatz einer WEP-Verschlüsselung sollte grundsätzlich verzichtet werden.

Auf Grund von aktuell bekannten Sicherheitslücken in so genannten „Consumer Produkten" sollten unternehmenstaugliche WLAN-Access-Points eingesetzt werden.

Die Nutzung externer Netzwerke sollte mit Bedacht erfolgen

Mitarbeiter, die nicht im Büro arbeiten und dort das Netzwerk nutzen können, sondern von unterwegs aus einen Zugriff auf die internen Daten benötigen, sollten diese externen Netzwerke mit Bedacht benutzen. Hierzu zählen öffentliche WLANs (Hotspots), Mobilverbindungen (WWAN) oder Netzwerke von Kunden bzw. Partnern.

In diesen Netzwerken herrschen in der Regel andere Sicherheitsniveaus als dies im internen Firmennetzwerk der Fall ist. So können beispielsweise Informationen, die über öffentliche Netzwerke übertragen werden, von anderen Teilnehmern oder auch dem Betreiber des Netzwerks gegebenenfalls mitgelesen werden.

Empfohlene Maßnahmen:
Die Auswahl und Verwendung betriebsfremder Netzwerke sollte mit Vorsicht erfolgen. Endgeräte, die über solche Netze mit dem Firmennetz kommunizieren müssen, sollten allen festgelegten Sicherheitsanforderungen genügen. Beispielsweise sollten je nach verwendetem Gerät ein aktuelles Virenschutzprogramm und eine Personal Firewall installiert und aktiviert sein. Bei der Übertragung von Passwörtern aus unsicheren Netzwerken heraus muss damit gerechnet werden, dass diese mitgelesen werden. Daher sollte eine Kommunikation ebenfalls nur über verschlüsselte Protokolle oder gar VPN-Verbindungen erfolgen.

2.4 Internet-Dienste und E-Mail

Für die meisten Benutzer mit Internetzugang sind E-Mail und Web-Browser die beiden wichtigsten Internetanwendungen. Kein Wunder, dass hier besonders viele Gefahren lauern. Durch das Herunterladen von Dateien können Schadensroutinen eingeschleppt werden, die gegebenenfalls nicht vom Virenschutzprogramm erkannt werden. Beim Surfen im Internet können unerwünschte Aktionen ausgelöst werden – vor allem dann, wenn riskante aktive Inhalte zur Ausführung zugelassen werden.

Beim Umgang mit Web-Browsern ist besondere Vorsicht geboten, riskante Aktionen sollten unterbunden werden

Die Verwendung von Web-Browsern stellt heute die wahrscheinlich häufigste Nutzungsform für den Zugriff auf Informationen im Internet oder bei Partnern dar. Die Zielsysteme sind in der Regel unbekannt und können Risiken und mögliche Schäden bei einem Zugriff hervorrufen. Oftmals werden auch eigene sensible Daten (z.B. Anmeldedaten oder Kreditkartendaten bei der Abwicklung von Kaufverträgen) an unbekannte Zielsysteme übertragen. Diese dürfen nicht durch unbekannte Dritte missbraucht werden.

Empfohlene Maßnahmen:
Im Unternehmen sollte ein Standard-Web-Browser definiert werden. Für diesen sollten mittels Konfiguration nur die aktiven Inhalte bzw. Skriptsprachen und Plug-Ins zugelassen werden, die für die Arbeit wirklich unverzichtbar sind. Besonders riskante Skriptsprachen (ORACLE JAVA, Microsoft ActiveX) sollten für Zugriffe auf unbekannte Web-Server deaktiviert werden. Der Standard-Web-Browser sollte im Rahmen des Patch-Managements regelmäßig auf allen Systemen aktualisiert werden. Sollte die Wahl des Standard-Web-Browsers nicht auf den Microsoft Internet Explorer fallen, sollte dieser dennoch an die geforderte Konfiguration angepasst und regelmäßig aktualisiert werden, da er auf Windows Systemen nicht deinstalliert und eine Nutzung nur mit zusätzlichem Aufwand verhindert werden kann.

Ein besonderes Augenmerk sollte auf die Verwendung von Technologien wie Adobe Flash und ORACLE JAVA gerichtet werden. Diese sollten im Rahmen des Patch-Managements immer die aktuellsten Sicherheitsupdates erhalten, da diese häufig Sicherheitslücken besitzen, die Angreifern ermöglichen, Schadcode in das System zu schleusen oder unerwünschte Funktionen auszuführen.

Die Übertragung von sensiblen Informationen sollte verschlüsselt (per HTTPS) erfolgen. Für die gesicherte Kommunikation mit Web-Servern verwendete Zertifikate müssen auf ihre Gültigkeit überprüft werden. Dazu muss das Zertifikat gültig (Anfangsdatum, Ablaufdatum, Servername, Hash) und die ausstellende Zertifizierungsstelle (vollständige Trustkette) vertrauenswürdig sein. Entsprechende Warnmeldungen dürfen durch Mitarbeiter nicht ignoriert werden. Auch der direkte Zugriff von außen auf interne Web-Server (beispielsweise Outlook Web Access) muss verschlüsselt erfolgen. Eingesetzte Zertifikate (vorzugsweise öffentliche Zertifikate) sollten ebenfalls auf ihre Gültigkeit geprüft werden. Warnmeldungen dürfen nicht ignoriert werden. Insbesondere bei Zugriff aus fremden unkontrollierten Netzwerken besteht hier die Gefahr eines Mitlesens durch Dritte (Man-in-the-Middle-Angriff). Insgesamt ist hier ist eine Mitwirkung der Mitarbeiter notwendig. Diese sollten über Risiken beim Zugriff auf unbekannte Web-Server und dem Umgang mit Warnmeldungen bei der Prüfung von Zertifikaten aufgeklärt werden.

Das Risiko einer ungewollten Ausführung von Schadcode kann technisch durch einen aktuellen Virenschutz, Angriffs- und Schadcode-Erkennung auf der Firewall oder den Einsatz geeigneter Schutzmechanismen wie Benutzerkontensteuerung (in aktuellen Windows Versionen) minimiert werden. Darüber hinaus bietet Microsoft aktuell mit dem Enhanced Mitigation Experience Toolkit (EMET) einen zusätzlichen Schutzmechanismus für den Internet Explorer. Auf Serversystemen sollte generell die Installation von Web-Browsern unterbleiben. Dafür besteht in der Regel (außer auf Terminal-Servern) keine Notwendigkeit. Für den Microsoft Internet Explorer selbst sollte die Enhanced Security Configuration aktiviert bleiben.

Protokolle mit Verschlüsselungsmechanismen für die Übertragung von E-Mails verwenden

E-Mails werden von Server zu Server oder zwischen Clients und Servern quer durch das Internet übertragen. Diese Übertragung kann von Angreifern abgefangen oder mitgeschnitten werden, die dadurch in den Besitz sensibler Informationen oder gar Anmeldedaten gelangen können. Dadurch ist ein Verlust der Vertraulichkeit oder gar der Integrität (Missbrauch der Anmeldedaten) gegeben. Aus diesem Grund sollte die Übertragung sämtlicher E-Mails an externe Server und der Zugriff auf interne Postfächer (mindestens von außen) ausschließlich verschlüsselt erfolgen.

Wenn Benutzer beispielsweise eine Web-Oberfläche (z. B. Outlook Web App) für den Zugriff auf ihr E-Mail-Konto verwenden, sollte hierbei auch der Zugriff verschlüsselt erfolgen, da ansonsten Anmeldedaten und E-Mails im Klartext übertragen werden.

Auch Übertragungsprotokolle wie IMAP4 oder POP3 dürfen für den Zugriff von außen nicht verwendet werden, da diese eine unverschlüsselte Übertragung von Anmeldedaten und Inhalten erlauben.

Empfohlene Maßnahmen:
Die Übertragung von E-Mails sowie der dazugehörigen Anmeldedaten und Passwörter sollte ausschließlich in verschlüsselter Form erfolgen. Server und Clients sind dazu so zu konfigurieren, dass eine unverschlüsselte Übertragung nicht möglich ist bzw. akzeptiert wird. Daher sollte auf Übertragungsprotokolle wie HTTPS, IMAP4-S, POP3-S und ESMTP zum Einsatz kommen.

Zusätzlich ist die Einführung einer generellen Signatur (Schutz der Integrität) oder eine Verschlüsselung (Schutz der Vertraulichkeit) von E-Mails mit S/MIME möglich. Diese ist aufgrund der notwendigen öffentlichen Zertifikate aufwändiger, kann aber zum Schutz von sensiblen E-Mails an externe Empfänger optional implementiert werden.

Bei E-Mail-Anhängen ist besondere Vorsicht notwendig

Von Schadcode in Dateianhängen oder Links empfangener E-Mails geht eine große Gefahr aus, wenn diese ungewollt ausgeführt werden. Kein Anwender darf solche Anhänge oder Links arglos ohne Überprüfung öffnen. In Zweifelsfällen sollte der Empfänger vor dem Öffnen eines Anhangs beim Absender nachfragen. Besonders tückisch ist, dass bestimmte E-Mail-Programme ohne Rückfrage beim Anwender direkt Anhänge öffnen und ausführen.

Empfohlene Maßnahmen:
Das automatische Öffnen von E-Mail-Anhängen kann durch Wahl eines E-Mail-Programms ohne diese Funktionalität, durch geeignete Konfiguration sowie durch Zusatzprogramme technisch verhindert werden.

Als Ergänzung zu der auf allen Clients vorhandenen aktuellen Virenschutzlösung können alternative Malware-Scanner auf den SMTP-Relays oder Firewalls eingerichtet werden. Auf diese Weise ist eine mehrfache Prüfung mithilfe unterschiedlicher Virenscanner möglich.

Eine Sensibilisierung aller Mitarbeiter zu sicherheitsrelevanten Aspekten beim Umgang mit E-Mails sollte erfolgen. Dabei sollten nicht nur E-Mail-Anhänge, sondern auch in den E-Mails enthaltene Links erwähnt werden, da diese ein hohes Gefahrenpotential haben.

Cloud-Dienste sollten nicht unbedacht und ungeprüft für vertrauliche Daten verwendet werden

Als Cloud-Dienste werden Lösungen bezeichnet, welche Dienste, Anwendungen oder Datenspeicher eines Anbieters über ein Netzwerk zur Verfügung stellen. Dabei läuft wahlweise die Anwendung oder der Dienst auf dem Server des Anbieters und nutzt das System des Anwenders nur als Ausgabegerät oder nur die Speicherung von Daten erfolgt auf dem Server des Anbieters. Public Cloud Services bieten solche Dienstleistungen einer offenen Benutzergruppe über das Internet an, während Private Cloud Services zumeist Dienstleistungsangebote an eine geschlossene Nutzergruppe über ein Wide Area Network (WAN; deutsch: Weitverkehrsnetz) oder das Internet darstellen.

Da bei Public Cloud Services Daten oder verarbeitende Anwendungen auf dem Server des Anbieters liegen, hat dieser weitgehende Möglichkeiten des Zugangs zu hinterlegten Daten. Der Anwender hat keine unmittelbare tech-

nische Kontrolle über die Sicherheit und Verwendung der Daten und Anwendungen und muss sich diesbezüglich auf die AGBs und Service Level Agreements des Anbieters verlassen, auf die er in der Regel keinen direkten Einfluss hat. Diese sind oft sehr allgemein gehalten und bieten zumeist keine sichere Grundlage für die Anforderungen an Vertraulichkeit, Integrität und Verfügbarkeit. Aufgrund des Zugriffs über das Internet sind Public Cloud Services zudem besonders exponiert und somit Gefahren durch Hacking oder Denial-of-Service-Angriffen ausgesetzt.

Viele Anbieter von Public Cloud Services machen keine Angaben darüber, in welchen Rechenzentren Daten gespeichert oder verarbeitet werden. Insbesondere bei weltweit tätigen Anbietern können diese teilweise oder vollständig in Ländern angesiedelt sein, deren Datenschutzbestimmungen nicht deutschen oder europäischen Standards entsprechen oder in denen staatliche Zugriffe auf verarbeitete Daten zulässig sind.

Empfohlene Maßnahmen:
Eine Nutzung von Public Cloud Services für die Verarbeitung oder Speicherung datenschutzrelevanter Daten ist nur dann zulässig, wenn der Service-Anbieter garantiert, dass die Daten nach deutschen oder europäischen Datenschutzbestimmungen verarbeitet werden und schlüssig dokumentieren kann, dass er hinreichend starke Verfahren etabliert hat. Es wird empfohlen, Datenspeicher von Public Cloud Service Anbietern nur zur Ablage oder zum Austausch von Daten zu nutzen, deren allgemeine Offenlegung unbedenklich ist.

Für die Übermittlung von sensiblen Daten zu Public Cloud Services sollte unbedingt eine dem Stand der Technik entsprechende sichere Verschlüsselung verwendet werden. Für die Ablage von sensiblen Daten in Public Cloud Services kann zudem eine dem Stand der Technik entsprechende sichere Verschlüsselung verwendet werden, deren Schlüssel lokal bei Anwendern gehalten und nicht über den Cloud Service verteilt werden. Technische und organisatorische Maßnahmen zur Verwaltung der Schlüssel sind vorzusehen.

Video- und Webkonferenzen sollten mit Bedacht verwendet werden

Präsentationen und Konferenzen werden bisweilen nicht mehr vor Ort, sondern online abgehalten. Dabei ersetzt eine Software, wie z. B. Cisco WebEx oder GoToMeeting Beamer und Whiteboard. Zuschauer oder Teilnehmer können ihre Clients via Internet miteinander verbinden und auf dem Bildschirm dargestellte Inhalte miteinander austauschen. Teilweise wird dabei zur Kommunikation der einzelnen Clients untereinander das unverschlüsselte HTTP-Protokoll verwendet und die Daten über einen dedizierten Server im Internet ausgetauscht. Da hierbei jeder teilnehmende Client unter Umgehung von Firewall-Mechanismen im Internet exponiert wird, stellt die Verwendung ein Risiko dar.

Viele Anbieter werben zwar mit der technischen Sicherheit ihrer Lösungen, allerdings bestehen selbst bei technisch sicheren Webkonferenzsystemen vielfältige Gefährdungen durch menschlich-organisatorische Faktoren.

Empfohlene Maßnahmen:
Ausnahmen in den Firewallregeln für teilnehmende Clients sollten mit Bedacht erfolgen. Anbieter öffentlicher Webkonferenzlösungen stellen Informationen zu den tatsächlich benötigten Protokollen und Ports zur Verfügung. Oftmals wird das unverschlüsselte HTTP-Protokoll nur als Fallback verwendet und wird bei einer Verbindungsmöglichkeit mit verschlüsselten Protokollen nicht benötigt.

Die Ausnahmen in den Firewallregeln sollten möglichst nach Abschluss der Webkonferenz deaktiviert und auf Anforderung vor Beginn einer neuen Webkonferenz wieder aktiviert werden.

Das gleiche gilt auch für Fernadministration von Systemen über das Internet (wie z. B. per TeamViewer).

Über VoIP sollten keine geschäftskritischen Informationen ausgetauscht werden

Unter dem Begriff Voice-over-IP versteht man das Telefonieren über Datennetzwerke, wobei Telefonie-Informationen wie Signalisierung und Sprachdaten übertragen werden. Häufig werden dabei öffentliche Netzwerke, wie z. B. das Internet genutzt, so dass eine sichere Kommunikation ohne besondere Maßnahmen nicht gewährleistet ist.

Bei der Nutzung von externen SIP-Gateways (Session Initiation Protocol) werden die VoIP-Daten ins Internet übertragen. Erfolgt dies unverschlüsselt, besteht die Gefahr, dass Gesprächsdaten von Unbefugten abgehört werden können. Es wird daher empfohlen, eine Lösung einzusetzen, welche die Verschlüsselung der VoIP-Daten unterstützt. Da vom Teilnehmer nicht festgestellt werden kann, ob auch alle anderen Kommunikationspartner über eine verschlüsselte VoIP-Verbindung verfügen, ist im Zweifel jedoch von einer unverschlüsselten Telefonverbindung auszugehen.

Bei der Nutzung proprietärer VoIP-Lösungen, wie z. B. Skype, VoIP-Buster oder Gizmo, ist zu beachten, dass der externe Datenverkehr schwer zu kontrollieren ist. Häufig werden nicht offengelegte Datenprotokolle sowie Peer-to-Peer Techniken eingesetzt, die eine Erkennung unerwünschter Kommunikation unmöglich machen.

Empfohlene Maßnahmen:
Über VoIP-Telefonate im Internet sollten keine geschäftskritischen Informationen ausgetauscht werden. Es wird empfohlen, auf eigenen SIP-Gateways bevorzugt auf etablierte offene Standards wie SIP over TLS/SSL und SRTP zu setzen.

2.5 Wartung von IT-Systemen

Software, die nicht auf dem aktuellen Update-Stand ist, stellt ein potentielles Sicherheitsrisiko dar. Oftmals gibt es bekannte und unbekannte Lücken oder Schwachstellen, die einen Angriff oder das Einschleusen von Schadcode ermöglichen.

Sicherheitsupdates müssen zeitnah eingespielt werden

Das regelmäßige und zeitnahe Einspielen von Sicherheitsupdates auf allen Systemen ist zwingend erforderlich, um die Ausnutzung von Sicherheitslücken in Kommunikationsmethoden, Scripting Engines oder anderen aktiven Softwarekomponenten zu unterbinden. Gleiches gilt analog für Hardware Appliances (wie Firewalls, Router, Switches etc.) mittels Einspielen von Firmware-Updates.

Empfohlene Maßnahmen:
Höchste Priorität bei Sicherheitsupdates haben angesichts der sich manchmal rasend schnell ausbreitenden neuen Schadsoftware die Virenschutzprogramme. Die Prüfung auf verfügbare Aktualisierungen und das Einspielen bei Verfügbarkeit sollte automatisch alle vier Stunden geschehen. Dafür sollte eine einheitliche Konfiguration des Virenschutzes auf allen Systemen erfolgen. Dies und die Überprüfung des Update-Standes kann durch den Einsatz einer zentralen Verwaltung für den Virenschutz erheblich vereinfacht werden.
Updates von Web-Browsern, E-Mail-Programmen und Betriebssystemen sollten ebenfalls regelmäßig, und zwar mindestens einmal pro Monat geplant, durchgeführt werden. Das betrifft auch Sicherheitsupdates für andere Anwendungssoftware und Firmware-Updates bei Verfügbarkeit. Sicherheitsupdates gegen sogenannte Zero-Day-Exploits sollten jedoch sofort bei Verfügbarkeit eingespielt werden.

Die Verteilung von Sicherheitsupdates in der eigenen Umgebung kann ggf. auch manuell erfolgen. Zentrale Patch-Management Lösungen bieten jedoch den Vorteil eines geringeren Aufwands bei der Verteilung von Updates, der Überwachung des Updatestatus, sowie der Sperrung von unerwünschten Updates.

Es sollte ein Prozess zum Einspielen erforderlicher Sicherheitsupdates erstellt werden

Selbst wenn der Systemverantwortliche wichtige Sicherheitsupdates nicht einspielt, bleibt deshalb weder automatisch das System stehen noch erfolgt umgehend ein bösartiger Hackerangriff. Das macht deutlich: Das Einspielen von Updates erfordert sehr viel Disziplin und muss von vornherein als Prozess verankert sein. Gerade bei Virenschutzprogrammen sollte das schnellstmögliche Einspielen von Updates zur Routine werden.

Empfohlene Maßnahmen:
Dafür sollte ein Konzept für das Patch-Management mit den dazugehörigen Richtlinien und Maßnahmen erstellt werden.

Für die Aktualisierung von Betriebssystemen und Programmen sollte ein Aktionsplan erstellt werden. Dieser sollte mindestens monatlich (an einem festen Tag, Patchday) die Installation von Updates vorsehen. Hierfür können – speziell für Server – Wartungsfenster definiert werden, in denen die kurzfristige Nichtverfügbarkeit von Servern (und damit auch deren angebotener Dienste) akzeptabel ist. Im Aktionsplan sollte festgelegt werden, wie der Patchday vorbereitet und durchgeführt (z.B. Reihenfolge der Server) wird.

Softwareänderungen sollten getestet werden

Theoretisch sollte jede Softwareänderung an Produktivsystemen zuvor ausgiebig in einer Testumgebung überprüft werden, damit nach erfolgter Änderung noch alle Systeme reibungslos funktionieren. Auch Updates von Virenschutzprogrammen haben bereits Unternehmensnetze lahmgelegt, da unternehmenseigene Software fälschlich als neuer Virus identifiziert und deaktiviert wurde.

Der Test von wichtigen Sicherheitsupdates erfolgt meistens unter besonderem Zeitdruck, da sie möglichst umgehend eingespielt werden müssen. In der Praxis müssen Administratoren daher besonders sorgfältig zwischen Sicherheitserfordernissen und den verfügbaren Ressourcen abwägen und vernünftige Kompromisse eingehen.

Empfohlene Maßnahmen:
Eine kurze Recherche über bekannte Probleme im Zusammenhang mit geplanten Sicherheitsupdates kann hilfreich sein. Auch die Verwendung von „Staging Systemen" ist möglich. Auf diesen (beispielsweise Arbeitsplätze der Administratoren) oder weniger wichtigen Servern werden Sicherheitsupdates vorab installiert, getestet und erst mit Zeitversatz für die anderen Systeme verfügbar gemacht.

Bei Wartungs- und Reparaturarbeiten sind besondere Vorsichtsmaßnahmen zu beachten

Dienstleister oder Servicetechniker (beispielsweise Techniker oder Vertreter des Herstellers bei Garantiefällen oder Supportverträgen) erhalten für Wartung- und Reparaturmaßnahmen Zugang zu sensiblen IT-Systemen und Informationen. Besonders wenn Computersysteme (oder auch einzelne Festplatten) repariert, ausgetauscht oder entsorgt werden, können Unbefugte (in der Regel auch noch auf defekten Datenträgern) vertrauliche Daten einsehen oder rekonstruieren.

Empfohlene Maßnahmen:
Dienstleister sollten generell vertraglich durch eine Erklärung zur Vertraulichkeit verpflichtet werden.

Servicetechniker sollten nie allein ohne Aufsicht an IT-Systemen arbeiten. Das bedeutet, dass eine Wartung oder Reparatur möglichst im Unternehmen erfolgen sollte. Wenn Computersysteme oder einzelne Festplatten das Haus verlassen, müssen vorher alle Daten sorgfältig gelöscht oder unlesbar gemacht werden. Um dabei eine Wiederherstellung zu verhindern, sollte die Löschung „sicher" erfolgen. Für alle gängigen Betriebssysteme gibt es Zusatzprogramme, die eine sichere Löschung von Datenträgern (beispielsweise Festplatten) beherrschen. Dabei wird der Datenträger mehrfach komplett überschrieben, was eine Wiederherstellung wirkungsvoll verhindert bzw. erschwert. Bei der Aussonderung von Datenträgern sollten diese physikalisch zerstört werden.

2.6 Verwendung von Sicherheitsmechanismen: Umgang mit Passwörtern und Verschlüsselung

Die Systeme müssen unsichere Passwörter vermeiden

Schlecht gewählte Passwörter stehen auf einer Hitliste besonders häufiger Sicherheitsdefizite ganz weit oben. Besonders Hacker nutzen diesen Umstand aus. Um sich gegen Hackerwerkzeuge zu schützen, die vollautomatisch alle möglichen Zeichenkombinationen ausprobieren oder ganze Wörterbücher einschließlich gängiger Kombinationen aus Zeichen, Worten und angefügten Zahlen testen, muss ein Passwort bestimmten Qualitätsanforderungen genügen. Es sollte nicht in Wörterbüchern vorkommen, nicht aus Namen bestehen (beispielsweise nicht von „Lieblingshelden" aus Literatur und Film) und auch Sonderzeichen oder Ziffern enthalten. Im letztgenannten Fall sollten allzu gängige Varianten vermieden werden, wie beispielsweise Anhängen einfacher Ziffern am Ende des Passwortes oder eines der üblichen Sonderzeichen „$, !, ?, #" am Anfang oder Ende eines ansonsten simplen Passwortes.

Empfohlene Maßnahmen:
Mit technischen Maßnahmen und deren Umsetzung mit Gruppenrichtlinien oder granularen Passwortrichtlinien können Parameter einheitlich bestimmt werden. Für den Fall, dass ein Passwort mehrmals hintereinander falsch eingegeben wurde, sollten kurzfristig weitere Anmeldeversuche verhindert werden (Account Lockout). Nach einer Sperre von wenigen Minuten ist dann wieder eine Anmeldung möglich. Dies verhindert ein automatisches fortlaufendes „Probieren" von Passwörtern per Wörterbuch- oder Bruteforce-Angriff durch Angreifer.

Als angemessene Parameter für die technische Umsetzung einer Passwortrichtlinie für alle Mitarbeiter mit einer Gruppenrichtlinie werden folgende Varianten empfohlen. Diese sollten allen Mitarbeitern vorgegeben werden.

Richtlinie	Variante 1	Variante 2
Maximales Kennwortalter	360 Tage	700 Tage
Minimales Kennwortalter	1 Tag	1 Tag
Minimale Kennwortlänge	12 Zeichen	15 Zeichen
Kennwortchronik erzwingen	24 Passwörter	Unendlich
Kontosperrungsschwelle	5 Versuche	15 Versuche
Zurücksetzungsdauer des Kontosperrungszählers	30 Minuten	30 Minuten
Kontosperrdauer	60 Minuten	60 Minuten
Kennwort muss Komplexitätsvoraussetzungen entsprechen	Aktiviert	Deaktiviert

Tabelle 2 – Passwortrichtlinien

Die Verwendung von Passwörtern für Systeme und Dienste, die nicht in der Domäne verwaltet oder sich sogar außerhalb des Unternehmensbefinden sollte durch organisatorische Maßnahmen bestimmt werden.

Bei besonders hohen Sicherheitsanforderungen können zusätzlich oder als Alternative zu den normalen Passwörtern biometrische Verfahren wie beispielsweise Fingerabdruckscanner, Smartcards oder Token (One Time Password Generator) zum Einsatz kommen.

Auf die Verwendung von Fotogesten (Picture Password) auf Clientsystemen ab Microsoft Windows 8 oder auf anderen mobilen Geräten mit Google Android sollte grundsätzlich verzichtet werden.

Für die „Erstellung" oder das „Merken" von Passwörtern kann auf entsprechende Hilfsmittel zurückgegriffen werden. Eine Reihe von kostenlosen Tools (beispielsweise KeePass, oder die Möglichkeiten des Betriebssystems) kann genutzt werden.

Es müssen gut gewählte (sichere) Passwörter eingesetzt werden

Die eigentlich sinnvolle Forderung, dass jedes Passwort in regelmäßigen Zeitabständen geändert werden sollte, macht das Dilemma offenkundig: Es ist schwer, sich alle Passwörter zu merken. Bis auf wenige Ausnahmen in Hochsicherheitsbereichen ist es daher legitim, sich seine Passwörter aufzuschreiben und an einem sicheren Ort aufzubewahren (aber natürlich nicht am Monitor oder in der obersten Schreibtischschublade [oder als unverschlüsselte Liste in gemeinsamen Unternehmensverzeichnissen]).

Problematisch ist auch die Gewohnheit, einheitliche Passwörter für viele verschiedene Zwecke bzw. Accounts zu verwenden. Gerät das Passwort einer einzelnen Anwendung in falsche Hände, so wird ein geschickter Angreifer dieses Passwort auch bei anderen Anwendungen derselben Person ausprobieren. Als Alternative empfiehlt sich hier das sogenannte Salting-Verfahren. Hierbei bleibt ein bestimmter Teil des Passworts unverändert und wird dann durch einige wenige zusätzliche Zeichen „gesalzen". Die daraus resultierenden Hash-Werte, mit denen Anmeldeverfahren üblicherweise arbeiten, sind dann völlig andere und damit nicht wiederverwendbar für eventuelle Angreifer.

Empfohlene Maßnahmen:
Eine oder mehrere (z.B. zusätzliche für Administratoren und Dienstkonten) Passwortrichtlinien sollten erstellt und umgesetzt werden. Diese sollten Angaben über die erforderliche Länge, einen notwendigen Wechsel, die notwendige Komplexität (Zeichenkombinationen), Hinweise für die Erstellung (Passwortgeneratoren, Salting) und den generellen Umgang mit Passwörtern (keine Weitergabe, sichere Aufbewahrung, Zurücksetzen) enthalten. Diese können in Form organisatorischer Maßnahmen (IT-Nutzungsrichtlinie) den Mitarbeitern zur Kenntnis gebracht werden. Besser ist hier jedoch die teilweise Bestimmung von technischen Maßnahmen und deren Umsetzung beispielsweise durch eine Windows Gruppenrichtlinie. Dadurch ist eine einfache Durchsetzung der Passwortrichtlinien für alle Mitarbeiter in der eigenen Umgebung möglich. Ab einem Domänenfunktionsebene (Functional Level) von „Windows Server 2008" sind auch granulare Passwortrichtlinien verfügbar, mit denen für unterschiedliche Benutzergruppen Vorgaben zu Passwörtern konfiguriert werden können. Besonders administrative Benutzer oder Dienstkonten sollten entsprechend lange und komplexe Passwörter verwenden.

Voreingestellte oder leere Passwörter sollten geändert werden

Bei der Erstellung von Benutzerkonten für neue Mitarbeiter werden oft zunächst Standardpasswörter hinterlegt. Auch manche Hard- und „Softwareprodukte verfügen im Auslieferungszustand über vordefinierte Benutzerkonten, deren Passwort leer oder immer gleich und allgemein bekannt ist. Viele Angreifer wissen das und probieren bei einem Angriffsversuch zunächst aus, ob vergessen wurde, diese Benutzerkonten mit neuen Passwörtern zu versehen.

Auch Dienstleister, die für einen externen Wartungszugang schlechte oder gar fest eingestellte Passwörter verwenden, sind ein Sicherheitsproblem. In Einzelfällen wurde bekannt, dass Hersteller nicht dokumentierte „Hintertüren" (engl.: Backdoors) in ihren Programmen installiert haben, beispielsweise um im Supportfall auf einfache Weise Administrationszugang zu erlangen.

Empfohlene Maßnahmen:
Neue Mitarbeiter sollten bei der ersten Anmeldung ihr Passwort gemäß Passwortrichtlinie individualisieren. Das lässt sich auch technisch erzwingen. Bei neu implementierten Hard- und Softwareprodukten sollte stets in den Handbüchern nachgelesen werden, ob solche Benutzerkonten vorhanden sind. Auch hier sollten voreingestellte oder bekannte Standardpasswörter grundsätzlich geändert und nicht zum Einsatz kommen.

Hersteller bzw. Dienstleister sollten explizit zusichern können, dass die oben beschriebenen Methoden nicht von ihnen angewandt werden.

Administrative Passwörter müssen sicher in der eigenen Umgebung verwahrt werden

Dienstleister besitzen als Einzige administrative Konten oder Kenntnis über eingesetzte Dienstkonten und deren Verwendung und Passwörter. Dadurch entsteht eine starke Abhängigkeit vom jeweiligen Dienstleister und erschwert bei dessen Ausfall eine Vertretung, einen Wechsel oder im einfachen Fall der Änderung von Passwörtern von Dienstkonten mit nicht absehbaren Folgen.

Empfohlene Maßnahmen:
Zu beauftragten Dienstleistern besteht in der Regel ein Vertrauensverhältnis, dass jedoch vertraglich abgesichert werden sollte. Mindestens ein administratives Konto (Windows Domäne) sollte im Besitz der FIRMA sein. Leider bestehen hier nur komplexe Möglichkeiten die Änderung des Passworts oder das Entfernen aus administrativen Gruppen (falls der Dienstleister über weitreichende administrative Rechte verfügt) zu verhindern. Deshalb sollte das Konto regelmäßig auf seine Funktionsfähigkeit überprüft und im Ernstfall für die Sperrung aller administrativen Konten des Dienstleisters verwendet werden.

Die Verwendung von Dienstkonten und anderen administrativen Konten (z.B. auf Appliances wie Firewall oder WLAN-Access-Points) muss dokumentiert werden. Informationen zu eingesetzten Konten und den dazugehörigen Passwörtern sollten in einem Passwortsafe innerhalb der FIRMA sicher verwahrt werden. Dieser muss regelmäßig gesichert werden. Mindestens einem Mitarbeiter der FIRMA sollte der Zugang zu diesem Passwortsafe bekannt und möglich sein.

Arbeitsplatzrechner sollten bei Verlassen mit Sperrbildschirm und Passwort gesichert werden

Jedes gängige Betriebssystem bietet die Möglichkeit, Tastatur und Bildschirm nach einer gewissen Ruhezeit zu sperren. Die Entsperrung erfolgt dann erst nach Eingabe eines korrekten Passwortes. Sperrbildschirme (bzw. Bildschirmschoner mit Passwortschutz) sollten benutzt werden, wenn unbefugte Dritte bei vorübergehender Abwesenheit des rechtmäßigen Benutzers Zugang zu dessen System erlangen könnten.

Empfohlene Maßnahmen:
Die Aktivierung der Sperre sollte nicht zu schnell erfolgen (sonst stört sie den Benutzer nach kurzen Bedienpausen). Ein häufig angewandter Zeitpunkt ist fünfzehn Minuten nach der letzten Benutzereingabe [und kann durch eine Gruppenrichtlinie erzwungen werden]. Zusätzlich sollte die Möglichkeit bestehen, im Bedarfsfall die Sperre sofort zu aktivieren (unter Windows findet sich diese Option nach Eingabe von Strg + Alt + Entf). Mitarbeiter sollten über die Möglichkeiten zum unmittelbaren Sperren beim Verlassen ihres Arbeitsplatzes informiert werden.

Sensitive Daten sollten verschlüsselt abgelegt werden

Spätestens dann, wenn jemand direkten Zugriff auf eine Festplatte mit sensiblen Daten erhält, sind unverschlüsselte Daten im Allgemeinen frei auslesbar. Die eingebauten Schutzmechanismen des Betriebssystems oder der jeweiligen Applikation beispielsweise durch die Vergabe von Berechtigungen bieten nur ungenügenden Schutz vor dem Zugriff durch Administratoren und Experten.

Empfohlene Maßnahmen:
Der Einsatz einer Verschlüsselungssoftware für vertrauliche Dateien sollte erwogen werden. Dafür stehen zahlreiche Produkte (teilweise auch kostenlos) oder Funktionen seitens des Betriebssystems – Windows BitLocker, Windows Encrypting File System (EFS) oder Microsoft Rights Management Services (RMS) – zur Verfügung und sollten für den Schutz von sensitiven Daten in dedizierten Ablageorten, von mobilen Datenträgern oder kompletten Systemen eingesetzt werden. Besonders bei Geräten, die die FIRMA verlassen (mobil arbeitende Mitarbeiter) oder Datenträgern, die sensible Daten enthalten, sollte eine Verschlüsselung zwingend eingesetzt werden.

Wie bereits beschrieben sollten Notebooks komplett verschlüsselt werden, weil sie besonders einfach gestohlen werden können.

Bei der Produktauswahl sollte darauf geachtet werden, dass die verwendeten Schutzmechanismen als sicher gelten.

2.7 Schutz vor Katastrophen und Elementarschäden: Datensicherung und Infrastruktursicherheit

Alle wichtigen Daten und Systeme müssen regelmäßig gesichert werden

Für die Datensicherung (Backup) stehen zahlreiche Software- und Hardwarelösungen zur Verfügung. Es ist wichtig, dass wirklich alle relevanten geschäftskritischen Daten vom eingerichteten Backup erfasst werden. Dies stellt insbesondere bei verteilten heterogenen Umgebungen eine besondere Herausforderung dar.

Empfohlene Maßnahmen:
Es sollte ein Backup-Konzept anhand der Fragen – „Was?" wird „Wie oft?" „Wann?" „Wohin?" und „Wie lange?" gesichert – erstellt werden. Auch hier sollte regelmäßig geprüft werden, ob alle geschäftskritischen Daten erfasst werden. Auch bei Einführung neuer Dienste sollte rechtzeitig an eine Aufnahme in das Backup gedacht werden. Oftmals sind hier zusätzliche Lizenzen, oder bei neuen Betriebssystemen sogar ein Update der Backup-Version oder schlicht eine Erweiterung der verfügbaren Backup-Kapazitäten notwendig.

Auch mobile Endgeräte wie Notebooks mit sensiblen Daten müssen mit einbezogen werden. Hier kann im einfachsten Fall eine automatische Synchronisation der Daten auf ein Serversystem erfolgen, dass Bestandteil der regelmäßigen Datensicherung ist.

In der Regel werden Backups zunächst auf Festplatten geschrieben und von dort für die Auslagerung auf Bänder kopiert. Dabei sollten die Backups insbesondere bei Nutzung von externen Festplattensystemen verschlüsselt werden.

Alle Anwender sollten wissen, welche Daten wann und wie lange gesichert werden.

Alle wichtigen Backups müssen regelmäßig eingespielt werden

Backups sind wertlos, wenn das Einspielen der Daten im Notfall nicht funktioniert. Daher sollte es ein Recovery-Konzept geben.

Empfohlene Maßnahmen:
Es sollte regelmäßig verifiziert werden, dass das Backup auch tatsächlich funktioniert und die Daten wieder erfolgreich eingespielt werden können. Es sollte eine tägliche Kontrolle der Backup-Protokolle erfolgen und bei Fehlern (Neustart oder Überarbeitung der Jobs) reagiert werden.

Alle wichtigen Backups müssen physisch ausgelagert werden

Backups sind nicht nur bei Problemen der IT-Systeme erforderlich, auch bei Elementarschäden helfen die Sicherungen, einen ordnungsgemäßen Betrieb schnellstmöglich wiederherzustellen.

Empfohlene Maßnahmen:
Die für die Auslagerung verwendeten Backup-Medien müssen an einem sicheren Ort, möglichst außerhalb des Unternehmens, aufbewahrt werden. Der Aufbewahrungsort sollte zudem hinreichend gegen Elementarschäden wie Feuer, Wasser und Ähnliches geschützt sein. Auch für den Transport dorthin sollten entsprechende Sicherheitsmaßnahmen ergriffen werden (Beauftragung zuverlässiger Mitarbeiter oder Dienstleister, Verschlüsselung der Backups, abgeschlossene Transportbox).

IT-Systeme müssen angemessen gegen Feuer, Überhitzung, Wasserschäden und Stromausfall geschützt sein

Nicht nur durch Fehlbedienung oder mutwillige Angriffe können einem Informationsverbund Schäden zugefügt werden. Oftmals entstehen gravierende Schäden infolge physischer Einwirkung von Feuer, Wasser oder Strom. Viele Geräte dürfen nur unter bestimmten Klimabedingungen betrieben werden. Daher sollten besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Router etc.) in ausreichend geschützten Räumen untergebracht werden. Zusätzlich sollten sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein.

Empfohlene Maßnahmen:
Im Serverraum sollte eine geeignete Löschanlage vorhanden sein, die für elektronische Geräte geeignet ist. Hier wären beispielsweise eine CO2-Anlage, ein entsprechender Feuerlöscher oder eine Nebelanlage (löscht mit vernebeltem destillierten Wasser) denkbar. Erstere beinhaltet allerdings den Nachteil, dass der Serverraum nach erfolgter Löschung zunächst aufgrund des Sauerstoffmangels schlecht betreten werden kann. Entsprechend sollte abgewogen werden, welcher Ansatz im jeweiligen Fall der Beste wäre.
Die Klimatisierung des Serverraums bzw. der Serverräume sollte nach Möglichkeit redundant ausgelegt sein, um bei einem Ausfall eine Überhitzung der Server und Komponenten – und damit ggf. einen Datenverlust – zu verhindern.
Die Stromversorgung der eingesetzten Server und anderer zentraler Komponenten sollte mithilfe einer Unterbrechungsfreien Stromversorgung (USV) gegen Stromausfall und Spannungsschwankungen abgesichert werden. Im Optimalfall sollte auch ein automatisches Herunterfahren von Serversystemen durch die USV bei längerem Stromausfall initiiert werden.

Maßnahmen zum Zutrittsschutz müssen umgesetzt werden

Auch kleine Unternehmen sollten sich Gedanken über den Schutz vor Einbrechern und anderen ungebetenen Gästen machen. Einige einfache Maßnahmen können bereits einen beträchtlichen Sicherheitsgewinn bringen. Es gilt zu überlegen, wo sich Besucher und Betriebsfremde in der Regel aufhalten und auf welche IT-Systeme sie dabei zugreifen könnten. Besonders Server oder Clients, mit denen auf sensitive Daten zugegriffen wird, sollten so aufgestellt sein, dass Fremde sich nicht unbemerkt an ihnen zu schaffen machen können. Auch Smartphones sollten nicht unbedacht herumliegen.

Die hier gegebenen Hinweise sind sicher nicht vollständig – sie sollten im Einzelfall überdacht und ergänzt werden.

Empfohlene Maßnahmen:
Besucher sollten nicht nur aus Höflichkeit aufmerksam betreut werden. Die Tätigkeit von Handwerkern, Servicetechnikern und Reinigungspersonal sollte bewusst geplant und allen Mitarbeitern bekannt gegeben werden.

Für die physische Sicherheit von Serversystemen oder auch zentralen Speichersystemen sollten bereits grundlegende Dinge wie z. B. eine stabile und möglichst feuerfeste Serverraumtür sowie eine elektronische (Transponder) oder physische (separater Schlüssel) Zugangskontrolle berücksichtigt werden.

Maßnahmen zum Schutz vor Einbrechern müssen umgesetzt werden

Auch kleine Unternehmen sollten sich Gedanken über den Schutz vor Einbrechern und anderen ungebetenen Gästen machen. Einige einfache Maßnahmen können bereits einen beträchtlichen Sicherheitsgewinn bringen. Es gilt zu überlegen, wo sich Besucher und Betriebsfremde in der Regel aufhalten und auf welche IT-Systeme sie dabei zugreifen könnten. Besonders Server oder Clients, mit denen auf sensitive Daten zugegriffen wird, sollten so aufgestellt sein, dass Fremde sich nicht unbemerkt an ihnen zu schaffen machen können. Auch Smartphones sollten nicht unbedacht herumliegen.

Empfohlene Maßnahmen:
Die Sicherheit des Büros ist durch eine polizeiliche Begehung auf Gefährdungen zu untersuchen, und geeignete Maßnahmen gegen Einbruch (Zäune, Schlösser an Jalousien etc.) sind zu ergreifen. Unter Umständen ist es sinnvoll, bestimmte Büros bei Abwesenheit der Mitarbeiter abzuschließen oder die Fenster (z. B. während der Mittagspause) nicht gekippt zu lassen

Das Unternehmen sollte durch eine Alarmanlage gesichert werden.

Der gesamte Bestand an Hard- und Software sollte in einer Inventarliste erfasst werden

Empfehlenswert ist eine Inventarliste, die regelmäßig aktualisiert wird. In vielen Fällen können diese Informationen aus den Buchhaltungsdaten entnommen werden. Doch selbst dann besteht oft Unklarheit über den letzten Standort oder darüber, ob ein vermisstes Objekt zu einem gegebenen Zeitpunkt schon länger fehlte oder erst vor kurzem abhanden kam. Auch Versicherungen benötigen Inventarlisten mit Wertangaben, damit im Schadensfall ordnungsgemäß reguliert werden kann. Anhand der Inventarliste kann darüber hinaus regelmäßig überprüft werden, dass keine Unterdeckung bezüglich der Versicherungssumme besteht.

Empfohlene Maßnahmen:
Hard- und Software sollte bei der Beschaffung in einer Inventarliste erfasst werden. Inventar sollte während des Lebenszyklus in der Liste gepflegt und bei Außerbetriebnahme entfernt werden. Siehe auch Sicherheitsmaßnahme zu „Herstellersupport".

3. Anhang

Die folgende Checkliste erlaubt den Status zur Grundsicherung schnell zu erfassen.

Informationssicherheitsmanagement

- ☐ Werden Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffungen von IT-Systemen und Anwendungen, Outsourcing- und Dienstleistungsverträgen)?
- ☐ Gibt es einen Handlungsplan, der Sicherheitsziele priorisiert und die Umsetzung der beschlossenen Sicherheitsmaßnahmen regelt?
- ☐ Sind für alle Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten (incl. Stellvertretung) festgelegt?
- ☐ Sind die bestehenden Richtlinien und Zuständigkeiten allen Mitarbeitern und relevanten Externen bekannt?
- ☐ Ist sichergestellt, dass es keine Ausnahmen (z.B. für Führungskräfte) gibt?
- ☐ Wird die Wirksamkeit von Sicherheitsmaßnahmen regelmäßig überprüft?
- ☐ Sind die Mitarbeiter über den Umgang mit vertraulichen Informationen am Arbeitsplatz ausreichend sensibilisiert?
- ☐ Werden bestehende Sicherheitsvorgaben kontrolliert, sind Konsequenzen bekannt und werden Verstöße geahndet?

Sicherheit von IT-Systemen

- ☐ Sind alle eingesetzten Soft- und Hardwareprodukte noch innerhalb des Herstellersupports?
- ☐ Sind alle Zertifikate noch mindestens 6 Monate gültig?
- ☐ Werden flächendeckend Viren-Schutzprogramme eingesetzt?
- ☐ Sind allen Benutzern Rollen und Profile zugeordnet worden?
- ☐ Gibt es einen Lebenszyklus-Prozess für Benutzerkonten?
- ☐ Gibt es verschiedene Rollen und Rechte für Administratoren?
- ☐ Werden Privilegien und Rechte von Programmen auf ein Minimum beschränkt?
- ☐ Werden sicherheitsrelevante Standardeinstellungen von Programmen und IT-Systemen geeignet angepasst?
- ☐ Werden Installations- und Systemdokumentationen erstellt und regelmäßig aktualisiert?
- ☐ Werden ausschließlich Systeme betrieben, die tatsächlich benötigt werden?
- ☐ Werden mobile Endgeräte über ein Mobile Device Management administriert?

Vernetzung und Internetanbindung

- [ ] Gibt es eine Firewall zum Schutz vor externen Zugriffen?
- [ ] Werden Konfiguration, Regelwerk und Funktionsfähigkeit der Firewall regelmäßig überprüft und kontrolliert?
- [ ] Gibt es ein Konzept, welche Daten und Dienste nach außen angeboten werden müssen?
- [ ] Greifen Dienstleister und Mitarbeiter ausschließlich über gesicherte Verbindungen von außen auf das interne Netz zu?
- [ ] Sind Netzwerkfreigaben nur für berechtigte Benutzergruppen eingerichtet?
- [ ] Sind WLAN, Netzwerkzugänge und Gästenetze angemessen abgesichert?
- [ ] Sind die Mitarbeiter über die Risiken der Nutzung von externen Netzwerken ausreichend sensibilisiert?

Internet-Dienste und E-Mail

- [ ] Sind Web-Browser und E-Mail-Programm sicher konfiguriert?
- [ ] Erfolgt die E-Mail-Übertragung ausschließlich über verschlüsselte Protokolle?
- [ ] Sind die Mitarbeiter im Umgang mit E-Mailanhängen ausreichend sensibilisiert?
- [ ] Sind die Mitarbeiter im Umgang mit Cloud Services ausreichend sensibilisiert?
- [ ] Wird für Videokonferenzen und Fernadministration (TeamViewer) ausschließlich https eingesetzt?
- [ ] Wird VoIP ausschließlich über verschlüsselte Protokolle eingesetzt?

Wartung von IT-Systemen

- [ ] Werden Sicherheitsupdates regelmäßig (1x pro Monat) und zeitnah (bei Zero-Days 1 Tag) eingespielt?
- [ ] Gibt es einen Patch-Management-Prozess und einen Verantwortlichen, der sich regelmäßig über Sicherheitseigenschaften der verwendeten Software und relevanter Sicherheitsupdates informiert?
- [ ] Werden die Softwareänderungen getestet, bevor sie allgemein eingespielt werden?
- [ ] Werden Servicetechniker beaufsichtigt und Datenträger bei der Entsorgung ausreichend gelöscht?

Passwörter und Verschlüsselung

- [ ] Verhindern die IT-Systeme die Verwendung unsicherer Passwörter?
- [ ] Sind die Mitarbeiter in der Wahl sicherer Passwörter ausreichend sensibilisiert?
- [ ] Werden alle voreingestellten oder leeren Passwörter geändert?
- [ ] Verfügt die Firma über eigene administrative Konten und Informationen für den Zugriff auf andere administrative Konten und Dienstkonten bei Dienstleistern?
- [ ] Werden Arbeitsplatzrechner bei Verlassen mit Sperrbildschirm und Passwort gesichert?
- [ ] Werden vertrauliche Daten und besonders gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

Datensicherung und Infrastruktursicherheit

- [ ] Ist bekannt, welche Daten für welches System wo gesichert und wie lange die Sicherungen aufbewahrt werden?
- [ ] Wird die teilweise oder vollständige Wiederherstellung regelmäßig getestet?
- [ ] Werden die Backups regelmäßig sicher ausgelagert und an einem sicheren Ort aufbewahrt?
- [ ] Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Spannungsschwankungen und Stromausfall?
- [ ] Ist der Zutritt zu wichtigen IT-Systemen und Räumen geregelt? Werden Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt?
- [ ] Besteht ein ausreichender Schutz vor Einbrechern?
- [ ] Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?