IT-Sicherheit für KMU
Ein Leitfaden

KMU ohne eigene IT-Abteilung tun sich oft schwer mit der IT-Sicherheit. Das zeigt eine Mitteilung des Nationalen Zentrums für Cybersicherheit (NCSC). Allzu oft werden banalste Sicherheitsvorkehrungen vernachlässigt oder vergessen.

Denn die Sicherheit der IT ist eine komplexe und aufwändige Aufgabe. Nur die wenigsten KMU sind in der Lage, sich selbst in der nötigen Tiefe um die Pflege der Systeme zu kümmern. Oft sind schlicht Versäumnisse oder Missverständnisse schuld daran, dass wichtige Sicherheitsmassnahmen nicht umgesetzt werden. Häufig lassen sich kleinere KMU von einem externen Partner beim Thema Informatik unterstützen. Sie verlassen sich darauf, dass dieser sich auch um die IT-Sicherheit kümmert. Das ist aber nicht automatisch der Fall. Bei der Zusammenarbeit ist es essenziell, dass der KMU-Verantwortliche weiss, was der Partner genau tut – und wo dessen Verantwortung aufhört. Dieser Leitfaden zeigt den Verantwortlichen in KMU, worauf sie ihr Augenmerk legen sollten, wie sie die Verantwortlichkeiten sauber klären können damit keine sicherheitsrelevanten Themen vergessen gehen und welche Fragen sie ihrem IT-Dienstleister unbedingt stellen sollten.

Virenschutz

Der Einsatz von Sicherheitssoftware (Antiviren-Software) gehört zu den wichtigsten Voraussetzungen für einen hohen Schutz des Unternehmensnetzwerks und der Unternehmensdaten.

Das reicht jedoch noch nicht aus. Die Systeme müssen regelmässig kontrolliert, auffällige Ereignisse interpretiert und entdeckte Fehler bearbeitet werden. Denn die automatisierten Sicherheits-Tools erkennen zwar viele Auffälligkeiten, Bedrohungen und Angriffe. Sie sind aber nicht in der Lage, immer alle Bedrohungen automatisch zu beseitigen. Die Installation von Virenschutz-Software ist also kein Grund, sich zurückzulehnen und sich um nichts zu kümmern. Erst die Verarbeitung von Warnmeldungen und die aktive Überwachung machen ein System sicher.

swisscom

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Ist auf allen PCs Antiviren-Software installiert und ist diese automatisch auf dem neusten Stand?
- Sind auch **NAS** bzw. Server entsprechend gesichert?
- Wie sieht es mit Smartphones und Tablets aus? Sind diese Geräte ebenfalls im Sicherheits-Dispositiv erfasst?
- Werden die Logfiles (hier werden sicherheitsrelevante Ereignisse aufgezeichnet) regelmässig geprüft und die entsprechenden Massnahmen ergriffen?
- Gibt es einen regelmässigen (z.B. einmal wöchentlich) System-Scan? Wer führt diesen aus und wer wertet das Resultat aus?
- Ist im E-Mail-Programm definiert, welche Anhänge als potenziell gefährlich gelten und sind diese Dateien gesperrt?
- Gibt es einen Notfallplan, wie bei einem Befall zu reagieren ist? Dies ist ein ganz wichtiger Punkt: Ihr Dienstleister muss fähig sein, nach einem Befall sofort zu reagieren und allenfalls verlorene Daten wiederherzustellen. Dieser Notfall sollte im Voraus geübt werden.

Datensicherung

Für sämtliche Geschäftsdaten müssen Sicherungskopien (**Backups**) erstellt werden, auf die im Falle eines Datenverlusts schnell und vollständig zugegriffen werden kann. Nur wenn ein Backup vom Unternehmensnetzwerk abgekoppelt und physisch an einem externen Ort aufbewahrt wird, ist ein Schutz gewährleistet. Wer also Beispielsweise seine Daten regelmässig auf ein externes Speichermedium ablegt und dieses dann auch an einem anderen Ort als dem Büro aufbewahrt, macht schon einiges richtig.

Einen grossen Nachteil hat diese etwas altmodische Art des Backups allerdings: Sie ist sehr schwerfällig und umständlich. Diesen Aufwand jeden Tag zu betreiben, will niemand auf sich nehmen. Speichert man seine Daten allerdings nur einmal wöchentlich, steigt das Risiko, wichtige Daten zu verlieren. Kommt dazu: Ein Schädlingsbefall wird unter Umständen erst nach Wochen festgestellt. Es ist also wichtig, auch länger zurückliegend gesicherte Daten zu haben.

Lokale Backups – oder auch manuell gesicherte Daten - reichen also nicht aus für eine sichere Datenhaltung. Automatisierte Backups in der Cloud bieten den höchsten Schutz. Backups via Cloud-Services haben den Vorteil, dass Sie keine teure und aufwändig zu betreibende IT-Infrastruktur erfordern. Bei besonderen rechtlichen Vorgaben sollten die Daten innerhalb der Schweiz gelagert werden.

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Wie sieht das Backup der Firmendaten aus? Wird dazu die Cloud benutzt oder befinden sich auch Server in Betrieb, dient ein **NAS** als Ablageort für die Unternehmensdaten? Werden gar noch PCs oder Festplatten für **Backups** verwendet?
- Wo werden die Backups gespeichert?
- In welcher Form sind die Daten gespeichert (verschlüsselt, komprimiert, allenfalls in einem speziellen Format)?
- Mit welcher Software werden die Backups angelegt und wie können Sicherungskopien wiederhergestellt werden?
- Wie weit zurück und in welchem zeitlichen Abstand können die Unternehmensdaten wiederhergestellt werden?
- Wer hat Zugriff auf die Backups?
- Wird das Backup regelmässig getestet? Dies ist ein wichtiger Punkt, den Sie unbedingt betonen sollten. Allzu oft stellt sich im Notfall heraus, dass das Backup nicht funktioniert.

Fernzugriff

Mitarbeitende müssen heute jederzeit auf Firmendaten und allenfalls auf Applikationen im Firmennetzwerk zugreifen können. Dateien lokal auf dem eigenen Rechner zu speichern, ist deshalb nicht zielführend. Damit Dateien allen Mitarbeitenden stets zur Verfügung stehen, sollten sie entweder in der Cloud oder auf einem eigenen im Firmennetzwerk zentral zugänglichen Server abgelegt werden.

Zentral ist dabei, diesen Zugriff von aussen gut abzusichern. Ein einfaches und bewährtes Mittel ist die so genannte **2-Faktor-Authentifizierung**: Ein sicheres Passwort bietet auch bei der Cloud-Anmeldung einen gewissen Schutz; doch mittels Keylogger – einer Malware, die Passworteingaben mitschneidet und dem Angreifer übermittelt – werden selbst ausgeklügelte Kennwörter schnell geknackt. Mit einer 2-Faktor-Authentifizierung können Anwender ihre Daten zusätzlich schützen: Für den Zugriff wird nicht nur ein Passwort, sondern ein zusätzlicher Code oder Schlüssel benötigt. Besonders verbreitet ist die 2-Faktor-Authentifizierung via Smartphone: Durch Ihre hinterlegte Handynummer erhalten Sie bei jeder Anmeldung eine SMS mit einem Zusatzcode, den sie in der Anmeldemaske eingeben müssen.

Die meisten Cloud-Anbieter bieten die 2-Faktor-Authentifizierung als zusätzliche Sicherheitsmassnahme an. klären Sie ab, ob auch Ihr Cloud-Provider über diese Funktion verfügt und richten Sie die 2-Faktor-Authentifizierung für alle Anwender ein.

VPN als sichere Verbindung: Viele Service-Provider ermöglichen eine Verbindung mittels VPN (virtuelles privates Netzwerk). Diese Tunnel-Verbindung ist sehr viel sicherer als der normale Internet-Zugriff über einen Browser.

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Wie ist der Fernzugriff auf Daten und Programme in der Cloud oder auf Firmenserver gelöst und wie ist dieser Zugriff gesichert?
- Gibt es die Möglichkeit, die Sicherheit des Fernzugriffs mit VPN zu erhöhen?
- Wurden die Benutzernamen und Passwörter beispielsweise im Server oder im NAS nach der Inbetriebnahme geändert?
- Werden die Passwörter regelmässig geändert?
- Wer hat Zugriff auf Benutzernamen und Passwörter?

Warn- und Fehlermeldungen

Sei es die firmeneigene **Firewall** als Absender, der Webbrowser oder der Internetdienstleister: Meldungen zur IT-Sicherheit bringen nur etwas, wenn sie der Benutzer auch ernst nimmt. In vielen Unternehmen nimmt man es damit nicht so genau: Warnhinweise am Computer werden oftmals ignoriert, weggeklickt oder totgeschwiegen. Und unter Umständen öffnen Benutzer damit einem Angreifer den Zugriff auf den eigenen Rechner und das Firmennetzwerk.

Bereits Ihr Webbrowser liefert wichtige Hinweise darauf, ob Sie sicher im Internet unterwegs sind: Websites mit einer sicheren Verbindung (SSL) werden beispielsweise durch ein Schloss-Symbol im URL-Eingabefeld gekennzeichnet – wie auch durch die URL, die mit «https://» (statt «http://») beginnt. Besuchen Sie ausschliesslich Seiten mit einer sicheren Verbindung. Damit verkleinern Sie das Risiko, dass Angreifer Ihre Verbindung «entführen» und für einen Angriff missbrauchen. Eine absolute Sicherheit bietet eine verschlüsselte Verbindung aber nicht. Denn Phishing-Seiten sind mittlerweile überwiegend auf gehackten Servern untergebracht, die über eine legitime verschlüsselte Verbindung erreichbar sind.

Darüber hinaus führt Google eine schwarze Liste für Webseiten und IP-Adressen, die gegen die Richtlinien der Suchmaschine, das Urheberrecht oder andere wichtige Gesetzesbestimmungen verstossen und die intensives Spamming betreiben. Diese Seiten entfernt Google aus ihrem Index und macht sie für Nutzer der Suchmaschine unauffindbar.

Neben Browser und Suchmaschine kann Sie auch Ihr Internet-Service-Provider vor gefährlichen Webseiten schützen. Swisscom setzt beispielsweise den Internet Guard ein, der auf Malware- oder andere gefährliche Websites hinweist, sofern ein Unternehmen einen Internetzugang von Swisscom nutzt.

⚠ Regeln befolgen: Für den richtigen Umgang mit Warnmeldungen sollten Sie folgende Richtlinien befolgen:

- Bleiben Sie auch bei vermeintlichen Warnmeldungen skeptisch. Überprüfen Sie Meldungen erst auf ihre Glaubwürdigkeit, bevor sie die darin genannten Handlungsempfehlungen wahrnehmen. Nehmen Sie im Zweifelsfall Kontakt mit dem Absender auf und lassen sie sich von ihm die Authentizität der Nachricht bestätigen – oder widerlegen.
- Halten Sie Ihren Browser aktuell. Aktuelle Browserversionen schützen besser vor Betrug, Datendiebstahl und anderen Sicherheitsbedrohungen. Deshalb sollten Sie und Ihre Mitarbeitenden die Update-Meldungen des Browsers keineswegs ignorieren, sondern Aktualisierungen so schnell wie möglich durchführen. Sorgen Sie mit Nachdruck für die Einhaltung dieser Regel.
- Informieren Sie ihre Mitarbeitenden über besonders schwerwiegende Meldungen. Sensibilisieren Sie Ihre Mitarbeitenden für Sicherheitshinweise und machen Sie deutlich, dass diese ernst zu nehmen und zu befolgen sind.

Netzwerk mit Firewall schützen

Der Datenverkehr im Netzwerk sollte mit einer **Firewall** geschützt werden. Eine solche Netzwerk-Firewall hat nicht viel mit der Software-Firewall zu tun, die bereits Windows mitbringt, diese schützt das Netzwerk nicht. Eine Netzwerk-Firewall überprüft nicht nur Daten, die hereinkommen als Schutz gegen Malware, sondern auch solche, die hinausgehen und verhindert so, dass sensible Daten gestohlen werden. Sie gewährt Schutz gegen Malware und bösartige Webseiten. Zudem umfasst dieser Netzwerkschutz auch Massnahmen für Geräte, die oft vergessen gehen, wie beispielsweise Netzwerkdrucker.

Um die nötige Sicherheit zu gewährleisten, empfiehlt es sich, Geräte wie Drucker oder PC's (Notebooks), Server, **NAS**, Bloginterna-of-things-Geräte wie Kassen, Maschinenanlagen etc. in eigene Netzwerksegmente einzubinden. Mit dieser Netzwerktrennung in sogenannte virtuelle Local Area Network (VLAN) können alle KMU eine Logik für Zugriffe auf Geräte definieren. Das kabellose Netzwerk (WLAN) ist ebenfalls Teil des Netzwerks. Zu den einfacheren Schutzmassnahmen gehört, für Besucher und Kunden ein separates WLAN anzubieten ohne direkte Verbindung auf wichtige Systeme des Unternehmens. Das kann verhindern, dass der verseuchte Rechner eines Gastes Schaden im Firmennetz anrichtet.

Eine Firewall korrekt einzurichten und zu betreiben, erfordert viel fachliches Know-how. Eine Managed Firewall, die vom IT-Dienstleister entweder vor Ort oder in der Cloud betrieben wird, ist oft die einfachste und günstigste Massnahme.

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Ist das Netzwerk mit einer Firewall gesichert?
- Sind auch NAS, Server und andere im Netzwerk eingebundene Geräte entsprechend gesichert?
- Ist es in meinem Betrieb nötig, segmentierte Netzwerke einzurichten?
- Wer überprüft die Firewall-Logfiles und wer veranlasst Massnahmen, falls nötig?
- Gibt es für Besucher ein eigenes, vom Unternehmen getrenntes Gäste-WLAN??

Patches und Updates

Hinzufügen von Software-Verbesserungen und Software Erneuerungen (Patches und Updates) sind zentrale Themen, wenn es um die Sicherheit Ihrer IT geht. Denn sehr viele dieser Nachbesserungen für das Betriebssystem oder auch normale Anwendungs-Software betreffen Sicherheitslücken. Eine der wichtigsten Massnahmen, um auf der sicheren Seite zu sein: Möglichst alle Updates für sämtliche Software möglichst schnell zu installieren. Grundsätzlich behebt ein Patch einen Fehler in der Software. Ein Update dagegen behebt mehrere Fehler und kann auch neue Funktionen in die Software implementieren.

Am wichtigsten ist dabei das Betriebssystem. Aufgrund der grossen Verbreitung ist Windows ein beliebtes Ziel für Hacker. Es gilt also, das Betriebssystem unbedingt immer auf der aktuellsten Version zu halten. Hier gilt ein besonders grosses Augenmerk auf Windows 7 zu legen, das in der Schweiz noch immer recht häufig verwendet wird. Wichtig zu wissen: Microsoft bietet seit dem 14. Januar 2020 keine Unterstützung und keine Patches mehr an für dieses Betriebssystem. Sollte also eine neue Sicherheitslücke auftauchen, wird diese von Microsoft nicht mehr geschlossen. Was Datendiebe natürlich freut.

Das Upgrade auf ein neues Betriebssystem hat allerdings seine Tücken. Möglicherweise läuft alte Hardware nicht mehr problemlos. Dieselbe Gefahr besteht auch bei alten Branchen-Lösungen auf Software-Seite.

Allerdings ist es damit noch nicht getan. Seien Sie sich bewusst, dass auch jede andere Software – und wirklich jede - ein potenzielles Sicherheitsrisiko darstellt. Sorgen Sie dafür, dass die restliche Software mit derselben Akribie gepflegt wird, wie das Betriebssystem. Je mehr unterschiedliche Programme auf Ihrem PC laufen, umso höher ist das Risiko einer Sicherheitslücke. Grundsätzlich gilt also: So wenige Programme wie möglich und so viele wie nötig. Beachten Sie dazu auch das Kapitel «Berechtigungen».

Sorgen Sie dafür, dass Ihre Hardware – zum Beispiel Drucker oder Webcams – regelmässig ein Update erfahren. Das heisst hier Firmware-Update und ist punkto Sicherheit genauso wichtig wie der Software-Patch. Denn all diese Geräte sind in Ihr Firmennetzwerk eingebunden.

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Welche Betriebssysteme werden in unserer Firma verwendet?
- Falls Sie Windows verwenden: Unterstützt Microsoft dieses Betriebssystem noch mit Sicherheits-Updates?
- Gibt es eine Übersicht über die verwendeten Programme in der Firma?
- Werden diese Programme regelmässig mit Updates versorgt? Ist gewährleistet, dass auch spezielle Branchen-Software immer auf dem neusten Stand ist?
- Ist gewährleistet, dass die Funktion «Automatisches Update» wo immer möglich eingeschaltet ist – und dass dieser Schritt von den Nutzern nicht übersprungen werden kann?
- Wird bei gefährdeter Hardware wie Drucker oder Webcam regelmässig die neuste Firmware aufgespielt?
- Bei einem Wechsel des Betriebssystems: Ist gewährleistet, dass Soft- und Hardware weiterhin problemlos funktionieren?
- Falls Sie eine Webseite oder einen Webshop betreiben: Wer sorgt dafür, dass auch diese stets auf dem aktuellen Stand sind? Ist das allenfalls ein anderer Dienstleister?
- Wie arbeitet hier ihr heutiger Cloudprovider bei Software-Angeboten und IT Infrastruktur-Lösungen im Bezug auf Updates und Patches?

Dateistruktur und Zugriffsrechte

Wer darf auf welche Daten zugreifen? Diese Frage müssen sich IT-Verantwortliche nicht nur aus Sicherheitsgründen stellen, sondern ganz auch wegen diverser gesetzlicher Vorgaben. Schliesslich sollen vertrauliche Zahlen oder Informationen nicht einfach jedermann zugänglich sein, auch nicht an sich vertrauenswürdigen Personen wie Ihren Angestellten

Der Teufel steckt aber im Detail. Zuallererst müssen Sie sich überlegen, wie Ihre Daten sinnvollerweise strukturiert sein sollten. Gerade, wenn die Daten – wie empfohlen – nicht einfach auf dem persönlichen PC gespeichert sind, sondern auf einem Server oder in der Cloud, sollten sie in einer logischen Struktur und mit einer nachvollziehbaren Namensgebung abgelegt sein. Der Grund: Nur wenn Daten wirklich klar strukturiert abgelegt sind, können diese für bestimmte Benutzergruppen freigegeben werden.

Eine saubere Dateistruktur von Grund auf zu entwickeln ist eine komplizierte Sache. Wir empfehlen, das gemeinsam mit einem Dienstleister zu erledigen, der auch gleich die passenden Speichermedien und Backup-Strategien entwickeln kann. Erledigen Sie diese Dinge immer gemeinsam und sprechen Sie Ihren Dienstleister auch auf die Dateistruktur an.

Zugriffsrechte sind ein wichtiger Eckpfeiler in einem IT-Sicherheitskonzept. Das hat einen einfachen Grund: Wer in Windows als «Administrator» geführt ist, hat das Recht, so genannte exe-Dateien auszuführen. Exe-Dateien sind im Grunde genommen alle Programme – auch die schädlichen. Häufig werden einem gefährliche exe-Dateien gut versteckt beispielsweise in Mails untergejubelt. Hat nun der Anwender oder die Anwenderin Admin-Rechte auf ihrem PC führt der Windows das Programm aus. Allerdings erst nach einer weiteren Anfrage, ob man das Programm XY tatsächlich ausführen wolle.

Eine sehr gute Sicherheitsmassnahme ist darum, dass möglichst wenige Personen im Betrieb diese Admin-Rechte überhaupt haben. Die meisten Mitarbeitenden sollten lediglich über eingeschränkte Rechte verfügen und können so von vornherein keine schädlichen exe-Dateien ausführen. Wenn ihre Firmen-PCs sauber vernetzt sind, sollten die einzelnen Mitarbeitenden keine Admin-Rechte haben. Wichtig ist, dass Sie diesen Punkt mit Ihrem IT-Dienstleister besprechen.

Je nach Betriebsart ist es für Angestellte ab und zu wichtig, auch andere Programme als Office zu nutzen. Erstellen Sie gemeinsam mit Ihren Kolleginnen und Kollegen eine Liste mit den erwünschten und benötigten Programmen. Diese Liste sollte in regelmässigen Abständen überprüft und angepasst werden. IT-Sicherheit und komfortables Arbeiten sollten sich nicht in den Weg kommen.

Diese Fragen müssen Sie Ihrem Dienstleister stellen:

- Wie sieht unsere Dateistruktur aus? Welche Daten werden wo und mit welcher Namenskonvention gespeichert? Erarbeiten Sie diese Struktur gemeinsam mit Ihrem Dienstleister, damit sie genau Ihren Bedürfnissen entspricht. Ein kompetenter Dienstleister wird Ihnen entsprechende Vorschläge machen.
- Wer hat Admin-Rechte in Windows – und warum?
- Welche Programme sind zur Nutzung freigegeben?
- Wie gehen wir mit neuen Bedürfnissen von Mitarbeitenden um? Wer entscheidet darüber, welche Programme ins Angebot eingebunden werden?
- Wer installiert neue Programme auf den Arbeitsstationen?
- Gibt es eine Möglichkeit, diesen Service zentral zu organisieren?

Handeln Sie jetzt!

Identifizieren Sie Sicherheitslücken in Ihrer IT und schützen Sie Ihr KMU vor Datenverlust und Angriffen. Wir unterstützen Sie gerne.

Jetzt telefonische Beratung anfordern

Glossar

NAS (Network Attached Storage)

Als NAS wird ein Netzwerkspeicher bezeichnet, der in einem Unternehmen oder auch zu Hause Speicherplatz für mehrere Benutzer zur Verfügung stellt. Anders als bei der Cloud bleiben die Daten stets beim Betreiber. Das NAS kann so konfiguriert werden, dass die Daten ausschliesslich innerhalb des eigenen Netzwerks oder aber übers Internet zur Verfügung stehen. Auf einem NAS lassen sich Daten verschlüsseln oder auf separaten Festplatten redundant speichern oder automatische Backups erstellen.

Logfiles

In Logfiles (oder auch Logdateien, Protokolldateien) protokolliert eine Software sämtliche Ereignisse, die in einem IT-System registriert werden. Damit können etwa im Netzwerk, auf Websites, im Betriebssystem oder im E-Mail-Verkehr alle Zugriffe, Fehler, Datentransfers oder Angriffe nachgewiesen werden. Eine Analyse der Logfiles bringt Erkenntnisse über Stabilität und Verfügbarkeit der Netzwerke, Systeme und Anwendungen.

Backup-Strategien

Grob kann in drei Backup-Strategien eingeteilt werden: Bei einem kompletten Backup erstellt eine Software jedes Mal eine vollständige Kopie der Daten. Diese Art der Datensicherung erfordert viel Speicherplatz und Zeit, eine vollständige Kopie der Daten lässt sich aber schnell wiederherstellen. Bei einem inkrementellen Backup werden nur jene Daten gesichert, die sich seit dem letzten Backup verändert haben. Es müssen weniger Daten gespeichert werden, doch wird die Wiederherstellung aufwendiger. Ein differentielles Backup wiederum kopiert alle seit dem letzten Backup veränderten Daten und speichert zusätzlich alle jene Daten, die sich seit dem letzten kompletten Backup geändert haben. Bei einer Wiederherstellung kann auf das vollständige Backup sowie auf das aktuellste Backup zugegriffen werden.

2-Faktor-Authentifizierung

Mit der 2-Faktor-Authentifizierung (2FA) oder auch Multi-Faktor-Authentifizierung (MFA) wird der Anmeldevorgang für persönliche Online-Konten oder IT-Systeme gesichert. Neben dem Abfragen von Benutzername und Passwort wird noch eine zusätzliche Komponente verwendet. Dies kann zum Beispiel ein per SMS an den Benutzer gesendeter Code sein. So wird verhindert, dass sich Unbefugte, die im Besitz von Benutzername und Passwort sind, einloggen können.

VPN

Eine VPN-Verbindung (Virtual Private Network) ermöglicht einen sicheren Zugriff auf ein Unternehmensnetzwerk (VPN) übers Internet. Dabei werden die Daten zwischen einem VPN-Server und dem Gerät des Benutzers verschlüsselt, sie befinden sich in einem sogenannten VPN-Tunnel und sind somit vor dem Zugriff oder der Manipulation durch Dritte geschützt.

Firewall

Eine Firewall kontrolliert den Datenverkehr, der in ein Netzwerk gelangt oder dieses verlässt. Per Filter-Einstellungen können Daten weitergeleitet oder blockiert werden. So können Netzwerke, Server, Betriebssysteme oder Geräte durch eine Firewall vor unerwünschten Zugriffen, Datendiebstahl oder dem Einschleusen von Malware geschützt werden. Eine Firewall kann sowohl eine Hardware-Komponente als auch eine Software sein.

Netzwerksegmentierung

Eine Segmentierung bzw. Unterteilung des Unternehmensnetzwerks erhöht die Sicherheit, indem einzelne Bereiche, Server oder Infrastrukturen voneinander getrennt werden. Die einzelnen Netzwerksegmente bleiben zwar verbunden, der Datenverkehr wird aber per Firewall kontrolliert. Als Alternative können zusätzliche virtuelle Netzwerke – sogenannte VLANs (virtual Local Area Network) – erstellt werden, die ebenfalls vom Unternehmensnetzwerk getrennt sind.