

dig it! GmbH

Gesellschaft für digitale Informationstechnologie



Security gefällig?

Die Managed Firewall
als Türsteher für Ihre IT!

Wir machen das für Sie!



Ihre IT benötigt Security? Dann engagieren Sie eine Managed Firewall!

Was ist eine Firewall?

Wortwörtlich übersetzt steht der Begriff Firewall für Brand-(schutz)mauer. Sie schützt sowohl Ihren privaten PC als auch Ihr Firmennetzwerk, indem sie den eingehenden und ausgehenden Datenverkehr analysiert. Konkret heißt das: Ihre Firewall prüft alles, was in Ihr Netzwerk hinein oder aus diesem heraus möchte, und gleicht diesen Datenverkehr mit definierten Regeln ab. Gleichzeitig schafft sie kontrollierte Übergänge, indem sie beispielsweise große Netzwerke in kleinere Bereiche untergliedert.

Zu kompliziert?

Sie können eine einfache Firewall auch mit einem Türsteher vergleichen. Minderjährige dürfen nicht in den Club hinein; Gäste, die noch nicht bezahlt haben, dürfen nicht hinaus. Der Türsteher behält all das im Blick und reagiert entsprechend. So auch die Firewall. Sie meldet Auffälligkeiten und

wehrt sie ab, Cyber-Attacken und andere Katastrophen können in Ihrem Netzwerk keinen Schaden anrichten.

Übrigens:

Das Konzept „Firewall“ ist alles andere als neu. Mittlerweile wird es seit mehr als 30 Jahren erfolgreich für die IT-Sicherheit eingesetzt und permanent weiterentwickelt.

Die Firewall: weit mehr als ein Türsteher

Firewalls sind also längst nicht mehr nur eine Zutrittskontrolle für Privatcomputer und Unternehmensnetzwerk. Die Funktionen sind viel umfangreicher geworden – und das müssen sie auch, da die Anforderungen an die IT-Sicherheit sowie Rahmenbedingungen wie das Home Office eine kontinuierliche Weiterentwicklung erfordern.

Die Vorteile einer Firewall

- + Umfassender Schutz vor webbasierten Angriffen auf Ihr Netzwerk
- + Absicherung des internen Datenverkehrs und der Internetanbindung
- + Klare Zugriffsregeln für Mitarbeiter und Spam-Filter
- + Einfache Einbindung von externen Filialen und Home-Office-Umgebungen via VPN-Verbindung

Mögliche Firewall-Funktionen

Umfangreiche Firewall-Lösungen setzen sich in der Regel aus Software- und Hardware-Bausteinen zusammen, die viele verschiedene Funktionen erfüllen. Im Zusammenspiel bilden diese Funktionen dann die Firewall Ihres Unternehmensnetzwerks. Indem Ihr Netzwerk in einzelne Segmente aufgeteilt wird, können Firewalls beispielsweise auch bestimmte Netzwerksegmente schützen. Im Falle einer Cyber-Attacke kann so der Schaden eingegrenzt werden – die Angreifer legen nämlich nicht Ihr gesamtes Unternehmen lahm. Weitere Funktionen können kontinuierliches Monitoring, Datensicherung und Backup-Lösungen sein. Sie sehen: Firewalls haben vielfältige Funktionen und übernehmen essenzielle Aufgaben für die IT-Sicherheit Ihres Unternehmensnetzwerks.

Übrigens: Unterschiedliche Funktionen sowie die Betreuung Ihrer Firewall durch einen IT-Dienstleister heißt im Fachjargon Firewall-Management bzw. Managed Firewall.

Wichtiger Baustein für Ihre IT-Sicherheit: das Firewall-Management

Mittlerweile ist Ihnen wahrscheinlich klar, dass eine einzige Firewall Ihre IT-Sicherheit nicht garantieren kann. Dafür benötigen Sie unterschiedliche Firewall-Funktionen, die

wiederum ein vollumfängliches Firewall-Management bilden: umfangreich, angepasst auf die Bedürfnisse Ihres Unternehmens und vor allem immer up to date. Denn eine veraltete Firewall-Lösung kann im schlimmsten Falle sogar mehr Schaden anrichten, da man sich auf der sicheren Seite wähnt. Wir raten Ihnen daher, vorzusorgen. Wie? Mit dem richtigen IT-Dienstleister an Ihrer Seite!

Wir übernehmen Ihr Firewall-Management

Setzen Sie bereits eine Firewall-Lösung ein, die aber dringend von einem Experten auf Herz und Nieren getestet werden sollte? Vielleicht möchten Sie in Sachen Firewall auch gern alles in die Hände unserer Experten legen und sich einfach nur auf Ihr Tagesgeschäft konzentrieren? Dann sind Sie mit einer Managed Firewall genau richtig.

Wir ermitteln die wichtigen Funktionen für Ihr Firewall-Management, richten Ihre Lösung voll funktionsfähig ein und stellen durch regelmäßige Überprüfungen sicher, dass Sie auf der sicheren Seite sind. Kontaktieren Sie uns – Ihren IT-Dienstleister – für mehr Infos. Wir unterstützen Sie gern!

Unser Firewall-Management enthält folgende Leistungen:

- + Bereitstellung von passender Hardware und entsprechenden Lizenzen
- + Einrichtung direkt vor Ort
- + Ständige Prüfung der Funktionsfähigkeit Ihrer Firewall
- + Laufende, automatische Aktualisierung der Firewall-Software
- + Virtuelles privates Netz (VPN) zur Einbindung von Home Office und Filialnetz
- + Auf Wunsch Ergänzung von Internetdiensten durch Inhaltsfilter

Wir machen das für Sie!



Als Fortune-Global-500-Unternehmen mit etwa 57.000 Mitarbeitern – vertreten in 180 Märkten rund um den Globus – hat sich Lenovo zur Aufgabe gemacht, Technologie ständig neu zu erfinden und die Welt damit interessanter zu machen. Das Produktportfolio des weltweit führenden PC-Unternehmens umfasst PCs, Tablets, Smartphones, Workstations, erweiterte und virtuelle Realität sowie intelligente Home-Office-/Office-Lösungen, Software, Dienstleistungen und Rechenzentrumslösungen.

Zuverlässige Partner für die alltäglichen Aufgaben



Intel® Core™ i5-1135G7 Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 8 MB Intel® Cache) | 8 GB RAM 256 GB SSD | Intel® Iris® Xe Grafik | Schnittstellen u. a. HDMI, Thunderbolt- und DisplayPort-Unterstützung über USB-C | Fingerprint-Reader | Integrierte Webcam-Abdeckung | Windows 10 Pro | 1 Jahr Herstellergarantie*

LENOVO THINKBOOK 15 G2
15,6" Full-HD-Display (39,6 cm, IPS, matt)
zzgl. gesetzl. USt.

729,00

LENOVO THINKBOOK 14 G2
14" Full-HD-Display (35,6 cm, IPS, matt)
zzgl. gesetzl. USt.

739,00



LENOVO DOCKINGSTATION DOCK USB-C GEN 2
Passend für die meisten Lenovo-ThinkPads | Schnittstellen u. a. HDMI, DisplayPort und USB-C | 3 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

159,00



PASSENDE
DOCKINGSTATION
GLEICH DAZU
KAUFEN



QHD-AUFLÖSUNG FÜR GESTOCHEN SCHARFE BILDER
LOW-BLUE-LIGHT-TECHNOLOGIE
HÖHENVERSTELL- UND NEIGBAR MIT PIVOTFUNKTION

LENOVO THINKVISION P24H
Auflösung 2.560 x 1.440 Pixel im 16:9-Format
Dyn. Kontrast: 3 Mio:1 | Helligkeit 300 cd/m²
Reaktionszeit 6 ms | HDMI, DisplayPort und USB-C
3 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

259,00



23,8" QHD
60,5 cm, IPS, matt



Home Office: eine Gefahr für Ihre IT-Sicherheit?

Keine Frage: Die Corona-Krise hat Deutschland einen Digitalisierungsschub verpasst. Ganz vorne mit dabei ist das Home Office. Vor der Pandemie von nur wenigen Unternehmen praktiziert, ist das Home Office nun zur Normalität geworden. Doch damit gehen nicht nur positive Entwicklungen einher. Das Home Office ist zum Beispiel zum neuen Spielplatz Cyberkrimineller geworden. Wir erklären, welche Gefahren vor allem die Heimarbeit mit sich bringt und wie Sie sich davor schützen können.

Cybercrime wird immer gefährlicher

Zu dem Schluss, dass Cybercrime immer gefährlicher wird, kommt das Bundeskriminalamt (BKA) in seinem „Bundeslagebild Cybercrime 2019“. Als besonders gefährlich gelten dort nach wie vor die bekannten Erpressertrojaner Emotet und Wannacry. Unternehmen, die Opfer eines Ransomware-Befalls wurden, hatten häufig mit einem längeren Produktionsausfall zu kämpfen. Nicht selten erwartete die Opfer aber auch der neue, aufwändige und kostspielige Aufbau des gesamten Unternehmensnetzwerks.

Brandbeschleuniger Home Office

Jetzt kommt noch das Home Office hinzu, das man geradezu als Brandbeschleuniger bezeichnen kann. Wieso ist das so? Zum einen waren die meisten deutschen Unternehmen im März 2020 nicht auf den plötzlichen Wechsel ins Home Office vorbereitet. Weder die IT-Infrastruktur noch die notwendigen Sicherheitskonfigurationen wurden den

eigentlich notwendigen Anforderungen gerecht. Zum anderen sorgten auch vielfältige Phishing-Angriffe dafür, dass Cyberkriminelle einige Erfolge verbuchen konnten. Der verringerte persönliche Kontakt zwischen Kollegen verschlimmerte das Problem sogar noch.

Fallstrick Remote-Desktop-Protokoll

Im Visier der Kriminellen steht besonders das Remote-Desktop-Protokoll (kurz RDP). Damit gemeint sind alle Arten von Remote-Desktop und Fernverwaltungssoftware (Microsoft, VNC, PC Anywhere oder Team Viewer), die das Steuern eines Computers aus der Ferne ermöglichen. Für Unternehmen stellt RDP eine beliebte Möglichkeit dar, aus der Ferne auf das Unternehmensnetzwerk zuzugreifen. Das Problem: Diese Verbindungen sind häufig schlecht geschützt und daher ein gefundenes Fressen für Cyberkriminelle – ein gelungener Angriff ermöglicht häufig den Zugriff auf das gesamte Unternehmensnetzwerk.

Home Office sicher machen – mit uns!

Die Corona-Krise und ihre Folgen werden uns noch einige Zeit begleiten – ebenso wie das Home Office. Höchste Zeit also, in die Home-Office-Sicherheit zu investieren und Ihr Netzwerk sicherer zu gestalten!

Wie? Mit uns! Wir freuen uns auf Ihre Kontaktaufnahme und beraten Sie gern.

Bestens ausgestattet für Ihr Business!



Fujitsu empfiehlt Windows 10 Pro für Unternehmen

STARKE KOMPONENTEN SORGEN FÜR EXZELLENTLE LEISTUNG

VERSCHIEDENE MODI FÜR MAXIMALE FLEXIBILITÄT IM MOBILEN EINSATZ

BIS ZU 12 STUNDEN AKKULAUFZEIT



Windows 10 Pro bedeutet Business.

FUJITSU LIFEBOOK U9310X

Intel® Core™ i5-10210U Prozessor (bis zu 4,20 GHz mit Intel® Turbo-Boost-Technik 2.0, 6 MB Intel® Cache) | Windows 10 Pro Display: 13,3" Full-HD, 33,8 cm, matt | 16 GB RAM | 512 GB SSD | Intel® UHD-Grafik | Card-Reader | Schnittstellen u. a. HDMI, DisplayPort- und Thunderbolt-Unterstützung über USB-C | LTE-fähig | Beleuchtete Tastatur | 2 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

1.599,00



STANDARD-LIZENZ FÜR DEN BETRIEB EINES SERVERS

MICROSOFT WINDOWS SERVER 2019 STANDARD 16-CORE
16-Core-Server-Lizenz | Geeignet für die meisten Infrastruktur-Szenarien

zzgl. gesetzl. USt.

639,00

PASSENDEN NUTZUNGS-LIZENZEN DIREKT DAZU KAUFEN

MICROSOFT WINDOWS SERVER 2019 DEVICE CALS¹ – 5 GERÄTE
Ermöglicht Zugriff auf den Server über 5 Geräte

zzgl. gesetzl. USt.

115,00

MICROSOFT WINDOWS SERVER 2019 USER CALS¹ – 5 BENUTZER
Ermöglicht Zugriff auf den Server für 5 Benutzer

zzgl. gesetzl. USt.

149,00

¹ CAL steht für Client Access License und bezeichnet die Lizenzen, die notwendig sind, um auf einen Server, der mit einem Betriebssystem desselben Herstellers ausgestattet ist, zuzugreifen.

Life Is On



USV: der Schutzengel für Ihre elektronischen Systeme

Zugegeben: Stromausfälle sind heutzutage eher selten. Doch wännen Sie sich nicht in trügerischer Sicherheit! Stromausfälle treten durchaus noch auf und schlagen dann mit beachtlichen Folgen zu Buche. Vor allem kleine bis mittelständische Unternehmen treffen Stromausfälle besonders hart, da sie während eines Stromausfalls in der Regel keine Umsätze generieren können. Sorgen Sie unbedingt vor!

Die technische Lösung, die Ihnen die Angst vor Stromausfällen nehmen kann, ist eine unterbrechungsfreie Stromversorgung (USV) von APC by Schneider Electric. Das Unternehmen bietet USV-Produkte an, die Ihre Computer und Peripheriesysteme, Netzwerk und Server sowie Datacenter und Anlagen im Falle des Falles schützen. Indem die USV die angeschlossenen, empfindlichen Systeme sofort mit sauberem Strom versorgt und sie vor Überspannungen schützt, fungiert Ihre USV-Lösung von APC als Schutzengel für Ihre elektronischen Systeme.

MIT LITHIUM-IONEN-TECHNOLOGIE



APC USV SMART-UPS 1HE LI-ION (SCL500RM1UC)

An Rack montierbar 1U | Leistungskapazität: 400 Watt / 500 VA
Anschlüsse: 4x IEC 60320 C13 und 1x IEC 60320 C14 | 230V Nominelle Eingangs- und Ausgangsspannung | RJ-45 und USB | 5 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

510,00

APC SMART-UPS 750 (SMT750IC)

Ausgangsleistungskapazität: 500 Watt / 750 VA | Anschlüsse: 6x IEC 320 C13 und 2x IEC Jumpers mit Netzausfallschutz | 230V Nominelle Eingangs- und Ausgangsspannung
Datenschnittstelle: SmartSlot, USB
3 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

289,00





Im Home Office an der langen Leine? Besser nicht!

Wir haben Ihnen im vorangegangenen Artikel bereits einige Gefahren vorgestellt, die das Home Office für Ihre IT-Sicherheit darstellt. Ein wichtiger Faktor zum Schutz Ihres Netzwerks – und da sind sich die Experten einig – ist es, Ihre Mitarbeiter auf eine sensible Internetnutzung hinzuweisen. So ließen sich laut „Bundeslagebild Cybercrime 2019“ des BKA bereits viele Gefahren vermeiden. Welche Regeln und Hinweise Sie Ihren Mitarbeitern geben sollten, lesen Sie hier.

Auf Cybercrime sensibilisieren

Manche Arbeitnehmer werden im Home Office abgelenkt und fallen so schneller auf Cyber-Attacken herein. Schulen Sie Ihre Mitarbeiter und kommunizieren Sie regelmäßig, worauf geachtet werden sollte und was die neuesten Angriffsstrategien der Cyberkriminellen sind.

WLAN-Netzwerke und private IT-Geräte

Weisen Sie Ihre Mitarbeiter darauf hin, regelmäßige Router-Updates durchzuführen und unbedingt ein neues, nicht standardmäßig vergebenes WLAN-Passwort zu definieren. Es bietet sich zudem an, Ihren Mitarbeitern zu Routern zu raten, die ein sicheres Verschlüsselungsverfahren nutzen. Legen Sie ebenso fest, dass Ihre Mitarbeiter keine privaten IT-Geräte wie Laufwerke oder USB-Sticks mit ihren Firmen-PCs verwenden und auch keine Verbindung zu Cloud-Diensten herstellen, die sie privat nutzen.

Vorsicht vor der Einsicht durch Dritte

Das Home Office ist nicht das Büro. Da Mitarbeiter häufig am Küchentisch oder im Schlafzimmer arbeiten, kann nicht ausgeschlossen werden, dass Dritte Einsicht in datenschutzrelevante Inhalte bekommen.

Betriebsübliche Arbeitszeiten einhalten

Auch im Home Office gelten die normalen Arbeitszeiten. Bitten Sie Ihre Mitarbeiter, diese weitestgehend einzuhalten, denn damit wird einerseits die Zusammenarbeit leichter, andererseits können so die üblichen Geschäftszeiten eingehalten werden.

Unterstützung gefällig?

Wir helfen Ihnen gern dabei, den Arbeitsplatz Ihrer Mitarbeiter im Home Office sicher zu gestalten. Selbstverständlich sind wir auch für Sie da, wenn Ihr Unternehmen bereits Opfer einer Cyberattacke geworden ist. Merken Sie sich jedoch: Vorsicht ist besser als Nachsicht. Warten Sie nicht, sondern kommunizieren Sie unsere Tipps schnellstmöglich an Ihre Mitarbeiter.



Kleine Multitalente



FUJITSU



MINI-PC FUJITSU ESPRIMO Q558

Intel® Core™ i5-9400T Prozessor (bis zu 3,40 GHz mit Intel® Turbo-Boost-Technik 2.0, 9 MB Intel® Cache) | Windows 10 Pro | 8 GB RAM | 256 GB SSD
Intel® UHD-Grafik 630 | Schnittstellen u. a. USB, DVI und DisplayPort
Abmessungen ca. 185 x 190 x 57 mm (BxTxH) | 1 Jahr Herstellergarantie*

zzgl. gesetzl. USt.

519,00



intel.



MINI-PC INTEL NUC

Intel® Core™ i7-10710U Prozessor (bis zu 4,70 GHz mit Intel® Turbo-Boost-Technik 2.0, 12 MB Intel® Cache) | 8 GB RAM | 256 GB SSD | Intel® UHD-Grafik 630 | Schnittstellen u. a. HDMI und Thunderbolt-Unterstützung über USB-C | Abmessungen ca. 117 x 112 x 38 mm (BxTxH) | Windows 10 Home | 3 Jahre Herstellergarantie*

zzgl. gesetzl. USt.

749,00

Stand 01/2021. Gültig bis 28. Februar 2021. Solange der Vorrat reicht. Irrtümer und Preisänderungen vorbehalten. Alle Preise sind Euro-Preise zzgl. gesetzl. USt.
Bildnachweise Adobe Stock: # 183487872 © LIGHTFIELD STUDIOS; # 233944822 © Shinonome Production; # 260666366 © goodluz; # 112922962 © fotogestoeber

dig it! GmbH

Gesellschaft für digitale Informationstechnologie



dig it! GmbH Gesellschaft für digitale Informationstechnologie | Neuenbaumerstraße 1 | 41470 Neuss
Telefon +49 2137 95340 | Fax +49 2137 953410 | E-Mail info@dig-it.org
Internet <http://www.dig-it.org>