Ein Unternehmen der

enviaM-Gruppe

enviaTEL

Whitepaper

Next Generation Firewalls – Eine Sicherheitslösung, die überzeugt.

Vorwort

Die Anforderungen an die Netzwerksicherheit wachsen enorm. Mit diesem Whitepaper wird aufgezeigt, was erforderlich ist, um die IT-Umgebung eines Unternehmens in Zukunft adäquat zu schützen.

Die aktuelle Netzwerksicherheitslage in Deutschland gilt als kritisch. Durch die stetig wachsende Digitalisierung, zuletzt durch die Covid-19-Pandemie, sind die Anforderungen an den Schutz unternehmensinterner Daten weiter gestiegen. Mit der zunehmenden Heterogenität von Netzwerken wird es für Unternehmen immer schwieriger, einen umfassenden Schutz zu erreichen und einen einheitlichen Überblick zu behalten. Die Komplexität dieser miteinander verbundenen Netzwerke führt häufig zu Fehlern oder Fehlkonfigurationen und macht sie anfällig für die sich ständig weiterentwickelnden Bedrohungen.

Herkömmliche Firewalls können den ansteigenden Ansprüchen an die IT-Sicherheit nur schwer gerecht werden. Die Vorteile einer Next Generation Firewall (NGFW) liegen hingegen klar auf der Hand: Diese vereint die Vorzüge anderer Firewalls und kompensiert deren Nachteile. Genaue Ausführungen und Erläuterungen dazu erhalten Sie im folgenden Whitepaper.

Inhalt

1. Aktuelle Bedrohungslage

„Erfolgreiche Cyber-Sicherheit ist unsichtbar. Nur wenn sie nicht funktioniert, wird sie sichtbar – als weltweiter Sicherheitsvorfall, als massiver Erpressungsversuch oder als Blockade und Ausfall von Systemen. Das schafft Aufmerksamkeit und macht Schlagzeilen, die eigentlich der Cyber-Sicherheit gehören sollte."[1] Mit diesen Worten hat Arne Schönbohm, Präsident des Bundesamts für Sicherheit in der Informationstechnik (BSI) einmal mehr die Notwendigkeit einer ausgebauten und zuverlässigen Informationssicherheit unterstrichen.

Durch das Bundesamt für Sicherheit in der Informationstechnik wird die Gefährdungslage in Sachen IT-Sicherheit in Deutschland genaustens untersucht. Dabei rücken vor allem Unternehmen sowie staatliche Institutionen in den Fokus. In vielen Teilbereichen der Informationssicherheit wird von der Alarmstufe Rot gesprochen. Dafür werden insbesondere drei Gründe hervorgehoben:

1.1 Grund 1: Deutliche Professionalisierung der Cyber-Kriminalität

Vor allem das Jahr 2021 haben Cyber-Kriminelle dafür genutzt, sich nicht nur neu zu positionieren und zu professionalisieren, sondern auch ihr Tätigkeitsfeld auszubauen. Daher ist es für KMU, Industrie und Behörden von äußerster Wichtigkeit, zu reagieren.

1.2 Grund 2: Zunehmende digitale Vernetzung

Durch die digitale Vernetzung wird der Austausch von Informationen zwischen Unternehmen mit Geschäftskunden und Dienstleistenden gefördert. Branchen, die ohnehin einen hohen Digitalisierungsgrad aufweisen, haben zudem ihre Prozesse innerhalb der Produktion oder Dienstleistungserstellung intensiver digital vernetzt. Es werden damit Schnittstellen zwischen Menschen, Technologien und Organisationen entwickelt.

1.3 Grund 3: Weite Verbreitung gravierender Schwachstellen in IT-Produkten

Die Gefährdungslage der IT-Sicherheit wird in Deutschland seit einigen Jahren bereits als hoch eingestuft. Eine Verringerung jener Gefährdungslage ist nicht absehbar. Viel mehr wird davon ausgegangen, dass diese in Zukunft weiter zunehmen wird. Im Februar 2021 wurden durchschnittlich pro Tag 553.000 neue Schadprogramm-Varianten erfasst. Das ist der höchste, jemals gemessene Wert.

1: Bundesamt für Sicherheit in der Informationstechnik (2021): Die Lage der IT-Sicherheit in Deutschland 2021. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=667A017CA28AEEDA52A78A3ACB69A15E.internet082?__blob=publicationFile&v=3, 18.07.22, 13:45 Uhr

Sich und sein Unternehmen vor Bedrohungen zu schützen, wird immer schwieriger. Besonders eine Schwachstelle im Microsoft Exchange-Server sorgte für negative Aufmerksamkeit. Bereits Anfang 2021 wurde durch die IT-Security Firma Volexity auffällige Netzwerkaktivitäten festgestellt. Microsoft stellte daraufhin im März sogenannte Out-of-Band-Updates zur Verfügung. Diese außerplanmäßigen Updates sollten die Schwachstellen in der Server-Anwendung Microsoft Exchange schließen. Betroffen waren Exchange-Server-Versionen von 2010 bis 2019. Microsoft sah die Bedrohung zunächst als gering an, jedoch entwickelte sich daraufhin eine aufsehenerregende Angriffswelle auf ungepatchte Exchange-Server-Instanzen durch die Hacker-Gruppe Hafnium.[2] Erst zum zweiten Mal seit dem Bestehen des BSI wurde die Warnstufe vier/rot, welche in der IT-Bedrohungslage als kritisch gilt, veröffentlicht und damit auf die Exchange-Server-Krise reagiert.

Darüber hinaus galt ein Cyber-Angriff auf Software-Supply-Chains als außerordentlich. Dabei nutzte die Angriffskampagne die Software Orion des amerikanischen Herstellers SolarWinds, um Unternehmen und Behörden zu kompromittieren. Auch wenn deutsche Ziele dabei weniger verfolgt wurden, stellt dieser Angriff einmal mehr die Risiken heraus, die durch jene Supply-Chain-Attacken entstehen. Angreifer infiltrierten in diesem Fall Malware in legitime Software-Produkte und damit in das Netzwerk des Herstellers. Durch ein hohes technisches Know-how der Angreifer konnte die Attacke erst sehr spät aufgedeckt werden. Seit Beginn der Covid-19-Pandemie ist zudem immer häufiger von

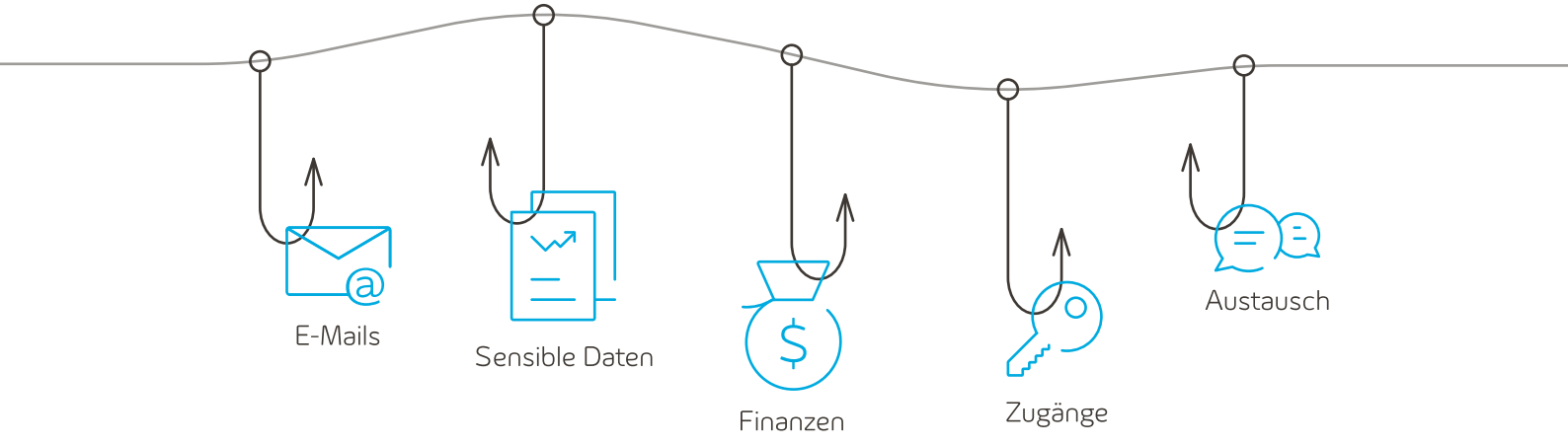


Abbildung 1: Folgenschwere Phishing-Kampagnen

2: Vgl. Volexity (2021): Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities. Zugriff: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/, 22.02.22, 14:00 Uhr

3: Vgl. Bundesamt für Sicherheit in der Informationstechnik (2021): Die Lage der IT-Sicherheit in Deutschland 2021. Zugriff: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2021.pdf;jsessionid=667A017CA28AEEDA52A78A3ACB69A1SE.internet082?__blob=publicationFile&v=3, 18.07.22, 11:00 Uhr

2.7 Warum sind herkömmliche Arten von Firewalls nicht mehr ausreichend?

In der Vergangenheit fungierte die Firewall als richtliniengesteuerter Kontrollpunkt, um den Netzwerkverkehr zuzulassen oder abzulehnen. Um in der heutigen digitalen Welt erfolgreich zu sein, müssen Unternehmen über bisher gängige Firewalls hinausdenken und neue Wege einleiten.

Durch die Weiterentwicklung der Anwendungsfelder, wie beispielsweise vermehrte Homeoffice-Tätigkeit und Remote Work, hat sich auch das Spektrum der Bedrohungen vervielfacht. Ein Großteil der Firewalls basiert auf Technologien, die vor modernen Internet-Anwendungen entwickelt wurden und daher weniger für den Umgang mit derzeitigen Risiken konzipiert sind. Der Aspekt der Kontrolle des gesamten Datenverkehrs spricht für den Einsatz von portbasierten Firewalls. Gängige Formen der Bedrohung werden zwar schnell und sicher erkannt, aber bei eingehendem Traffic werden Angreifer nicht daran gehindert, Attacken über geöffnete Ports auf die dahinterliegenden Webserver/Applikationen durchzuführen.

Eine herkömmliche Firewall ist für Angriffe auf Applikationsebene ebenfalls blind. Die heutige Netzwerksicherheit muss deshalb die jeweiligen Dienste und den dazugehörigen Kontext erkennen. Früher konnte man Dienste einfach anhand des Ports unterscheiden (Port 21 = FTP, Port 80 = http etc.) Heute läuft aber ein Großteil des Datenverkehrs über die Ports 80 (unverschlüsseltes http) oder 443 (https). Zudem werden Daten über weltweit verteilt ausgeliefert. Man kann so Dropbox nicht von Youtube oder normalen Webseiten unterscheiden. Deshalb müssen die Daten genauer untersucht werden. Bei verschlüsseltem Verkehr ist dieser vorher zu entschlüsseln (Deep Paket Inspection). Dies schließt Anwender, Session, URL, Schadcode, sensible Inhalte u.v.m. ein. Nur so können entsprechende Gegenmaßnahmen in die Wege geleitet werden.

Viele Unternehmen haben in den letzten Jahren Möglichkeiten ausprobiert, ihre Firewalls durch weitere Strategien wie beispielsweise Antivirus-Gateways, die einen Echtzeitschutz vor bekannten Viren und Trojanern versprechen, Intrusion Prevention Systeme (IPS), die Angriffe erkennen und diese selbstständig abwehren, oder auch Webfilterprodukte zu verschärfen und umso sicherer zu gestalten. Durch fehlende Einblicke in den gesamten Datenverkehr kann jedoch nicht gewährleistet werden, dass tatsächlich alles geprüft wird, was Gefahrenpotenziale bietet.

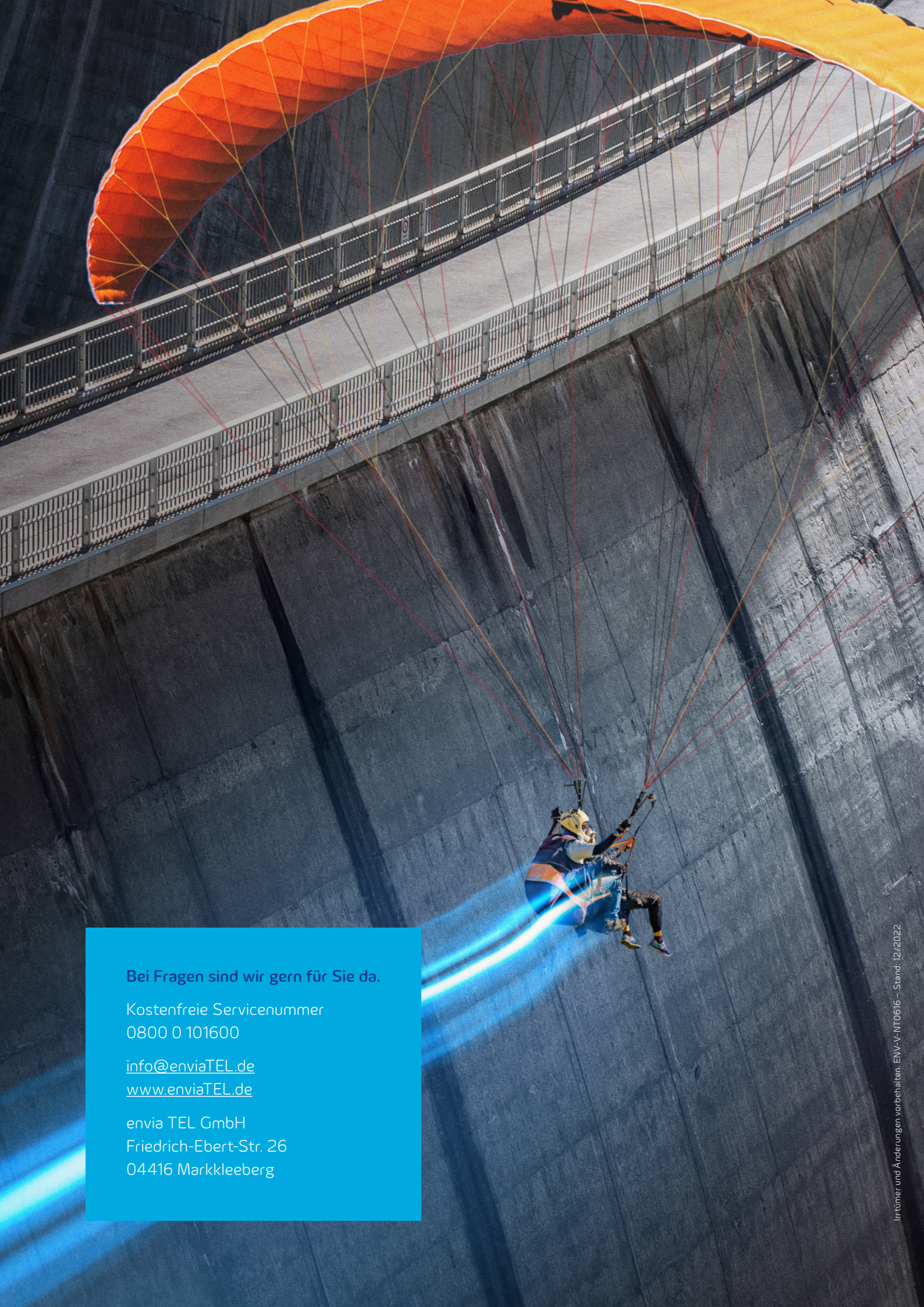
3. Next Generation Firewall (NGFW) – die Zukunft der Sicherheitstechnologie?

Wünsche und Ansprüche nach einer allumfassenden Sicherheitslösung sind groß – durch die pandemiebedingten Anforderungen an die Digitalisierung wurde dies noch einmal verschärft. Benötigt wird eine Art Update, eine Weiterentwicklung der Standard-Firewalls, die unter anderem Datenanalysen auf der Anwendungsebene ermöglicht. Verwirklicht werden kann dies durch Next Generation Firewalls, abgekürzt NGFW.
Bei einer NGFW handelt es sich um ein Netzwerksicherheitsgerät, das Funktionen bietet, die über eine herkömmliche, Stateful Firewall hinausgehen. Während eine herkömmliche Firewall in der Regel eine zustandsabhängige Prüfung des ein- und ausgehenden Netzwerkverkehrs gewährt, umfasst eine Next Generation Firewall zusätzliche Funktionen wie Anwendungserkennung und -kontrolle, integrierte Intrusion Prevention, wobei Angriffe auf Netzwerke oder Computersysteme erkannt und automatisch abgewehrt werden, sowie Cloud-basierte Bedrohungsdaten. Generell können NGFW Unternehmen – von KMUs bis hin zu Großunternehmen – folgende fünf Vorteile verschaffen.[14]

3.1 Vorteil 1: Weniger Cyberangriffe, dafür erweiterte Sicherheit

Die wichtigste Aufgabe einer Firewall ist es, Sicherheitsverletzungen zu verhindern und Unternehmen zu schützen. Da vorbeugende Maßnahmen jedoch nie vollumfänglich wirksam sein können, sollte eine Firewall auch über Funktionen verfügen, die fortschrittliche Malware schnell erkennt, wenn sie vordere Verteidigungslinien umgeht. Folgende Punkte einer Firewall sollten deshalb erfüllt werden:

- **Prävention!**
  Angriffe werden gestoppt, bevor sie ins Innere gelangen.
- **Erstklassiges Intrusion-Prevention-System!**
  Versteckte Bedrohungen werden somit erkannt und schnell gestoppt.
- **URL-Filterung!**
  Diese setzt Richtlinien für Millionen URLs durch.
- **Integriertes Sandboxing und fortschrittlicher Malware-Schutz!**
  Das Verhalten unbekannter Dateien wird durch das Ausführen in einem getrennten System (Sandbox) analysiert – und das bevor die Datei ausgeliefert wird.
- **Erstklassige Threat Intelligence-Organisation!**
  Diese sammelt Daten aus verschiedenen Quellen und stellt sie in aufbereiteter Form der Firewall zur Verfügung, um neue Bedrohungen zu stoppen.[15]



Bei Fragen sind wir gern für Sie da.

Kostenfreie Servicenummer
0800 0 101600

info@enviaTEL.de
www.enviaTEL.de

envia TEL GmbH
Friedrich-Ebert-Str. 26
04416 Markkleeberg