UNTERSCHÄTZTES IT-SICHERHEITSRISIKO:

Warum UTM-Appliances Betriebe unzureichend schützen

Vor zehn Jahren waren Unified-Threat-Management-(UTM)-Lösungen perfekt, um die IT von KMUs zu schützen. Heute entwickelt sich das lokale Appliance-Modell zu einer Gefahr, weil sie die Angriffsfläche für Cyberkriminelle vergrößert. Ursachen und eine Alternative | VON THOMAS HEFNER

Ein einheitliches Bedrohungsmanagement läßt sich mit einer Box erreichen. Mit diesem Versprechen wurden 2007 die ersten UTM-Appliances eingeführt, die dieses mit einer damals fortschrittlichen Firewall und zusätzlichen All-in-One-Sicherheitsfunktionen erfüllten. Ein solches Gerät stellt Features wie Anti-Virus, Anti-Spyware, Anti-Spam, Netzwerk-Firewall, Angriffserkennung und -Überwachung sowie Inhaltsfilter an einem einzelnen Punkt im Netzwerk bereit. Der Ansatz überzeugte insbesondere KMU. Der Vorteil von UTM-Geräten entwickelt sich allerdings schnell zum Nachteil: Versagt die Hardware, stellt sie eine zentrale Schwachstelle dar, die existenzbedrohende Datenpannen oder Cyberattacken nach sich ziehen kann. Denn ein lokales KMU-Appliance-Modell weist potentiell Sicherheitslücken auf.

1. Nur zeitweise Schutz einiger Nutzer: Herkömmliche UTM-Appliances schützen lediglich die Server und Arbeitsgeräte, die sich im Büro befinden. Deren Anzahl nimmt ab, während immer mehr Laptops, private Geräte, Smartphones und Tablets zwischen Heim- und Unternehmensnetzwerk hin und her wechseln. Gerade hier sind ungeschützte Einfallstore, ebenso wie bei anderen Personen, die Zugang zum Unternehmensnetzwerk haben.

2. Schutz für wenige Daten: KMU setzen verstärkt auf Cloud-Anwendungen von Drittanbietern wie Office 365, Salesforce, Box und viele hunderte mehr. Ihre Unternehmensdaten sind dadurch auf mehreren Servern und Cloud-Rechenzentren verteilt. 5G-Technologien werden den Trend zu dezentralen, Cloud-basierten Rechenzentren beschleunigen. Eine lokale UTM-Appliance schützt dann nur noch die lokal gespeicherten Unternehmensdaten.

3. Deaktiviertes Feature und fehlende Expertise: UTM-Geräte verfügen über eine SSL/TLS-Entschlüsselungsfunktion. In der Praxis wird diese jedoch in neun von zehn Fällen ausgeschaltet, um Performanceprobleme zu vermeiden. Die Folge: Eine Sicherheitslücke entsteht, wodurch das Netzwerk fast vollständig offensteht, weil wie der meiste Geschäftsverkehr auch die Sicherheitsbedrohungen heute verschlüsselt sind. >>

Bild: da-kuk via Getty Images

IMPRESSUM

Computern im Handwerk/ handwerke.de
gegründet 1984, dient als unabhängiges Fachmagazin für moderne Kommunikation den Betrieben der **Bauhaupt- und Nebengewerbe** im „portionierten" Wissens- und Technologie-Transfer.

Herausgeber: Horst Neureuther

CV Computern-Verlags GmbH
Goethestraße 41, 80336 München

Telefon 0 89/54 46 56-0
Telefax 0 89/54 46 56-50
Postfach 15 06 05, 80044 München
E-Mail: info@cv-verlag.de
redaktion@cv-verlag.de
www.handwerke.de

Geschäftsleitung:
Dipl.-Vw. H. Tschinkel-Neureuther

Anzeigenleitung:
Dipl.-Vw. Heide Tschinkel-Neureuther
e-mail: anzeigen@cv-verlag.de

Redaktion und redaktionelle Mitarbeiter in dieser Ausgabe:
Nicky Giebenhain, Thomas Hefner, Jens Kathmann, Björn Lorenz, Roswitha Menke, Nadja Müller, Horst Neureuther (verantw.), Christian Paulus, Gundo Sanders

Anzeigenvertretung:
Medienmarketing SANDERS
Tel. 0 72 03/50 27 270
Mail: gsanders@mm-sanders.de

Layout:
AD&D Werbeagentur GmbH,
Silvia Romann, Dietmar Kraus

Druck:
Walstead NP Druck GmbH, St. Pölten

Druckauflage: 52.500
Tatsächliche Verbreitung: 51.412 (III/20)
Auflage und Verbreitung kontrolliert.

36. Jahrgang
Erscheinungsweise: 10 x jährlich

Abo-Preis:
29,– € p.a. plus Porto inkl. MwSt.

Einzelpreis: 2,90 €
Ein Abonnement verlängert sich automatisch um ein Jahr, wenn es nicht spätestens 3 Monate vor Ablauf des Bezugszeitraumes gekündigt wird.

ISSN 0931-4679
Mitglied der Informationsgemeinschaft zur Feststellung der Verbreitung von Werbeträgern e.V. (IVW) Berlin

Zur Zeit gilt die Anzeigenpreisliste Nr. 38 vom 01.11.2020.

Titelkopf: © Fotolia.de/yellowj

Aktion:
34,90[1] €
statt 49,90 €
für 24 Monate

Gutes Internet war noch nie so wichtig

Jetzt wechseln und bis zu 1000 Mbit/s[2] sichern

Mit dem Kabel-Glasfasernetz von Vodafone ist Ihr Business für alles bereit.

vodafone.de/businesscable

Ihr Anschluss-Service:
Umstellung ohne Ausfallrisiko mit Vor-Ort-Installation

Ihre exklusiven Business-Vorteile:
Neueste Fritz!Box[3], Mobile Flat[4], feste IP-Adresse inklusive[5]

Ihr persönlicher Geschäftskunden-Service:
Wir sind rund um die Uhr für Sie da

Ready?

vodafone business

1 Red Business Internet & Phone Cable kostet im Aktionszeitraum 21.10.2020 – 20.01.2021 (Verlängerung vorbehalten) in der Bandbreite 500 34,90 € statt 44,90 € in den ersten 24 Monaten monatlich (ab dem 25. Monat 64,90 € monatlich) und in der Bandbreite 1000 34,90 € statt 49,90 € in den ersten 24 Monaten monatlich (ab dem 25. Monat 69,90 € monatlich). Alle Preise sind Nettopreise. Im Aktionszeitraum entfällt zudem für alle Tarife das einmalige Bereitstellungsentgelt von 69,90 € (83,18 € inkl. MwSt.). Gültig für Internet- & Phone-Neukunden sowie für Kunden, die in den letzten 3 Monaten keine Internet- und/oder Telefonkunden der Vodafone BW GmbH, Vodafone Hessen GmbH, Vodafone NRW GmbH, Vodafone Kabel Deutschland GmbH bzw. der Kabel Deutschland Vertrieb und Service GmbH waren. Mindestlaufzeit 24 Monate. Verlängerung um jeweils 12 Monate, wenn nicht 12 Wochen (hiervon abweichend 3 Monate in BW, Hessen und NRW) vor Laufzeitende in Textform gekündigt wurde. 2 Beachten Sie bitte die Verfügbarkeit: Die Höchstgeschwindigkeit von 1000 Mbit/s ist in ersten Städten und Regionen unserer Kabel-Ausbaugebiete und mit modernisiertem Hausnetz verfügbar. Weitere Standorte folgen. Prüfen Sie bitte, ob Sie die Produkte im gewünschten Objekt nutzen können. 3 Das erforderliche Endgerät wird während der Vertragslaufzeit zur Nutzung überlassen und ist nach Vertragsende zurückzugeben. Modelländerungen vorbehalten. 4 Kostenlose Telefonate ins deutsche Fest- und Mobilfunknetz. Sonderrufnummern ausgenommen. Telefonate ins Ausland, z. B. USA, ab 8,32 ct/Min. (9,9 ct inkl. MwSt.). Call-by-Call und Preselection nicht verfügbar. 5 In den Tarifen Red Business Internet & Phone 500 oder 1000 Cable ist eine feste IP-Adresse kostenlos inklusive. Anbieter in NRW: Vodafone NRW GmbH, in Hessen: Vodafone Hessen GmbH & Co. KG, in BW: Vodafone BW GmbH: Aachener Str. 746–750, 50933 Köln. Anbieter der übrigen Bundesländer: Vodafone Kabel Deutschland GmbH, Betastr. 6–8, 85774 Unterföhring.

Ohne SSL/TLS-Inspektion sind alle anderen Sicherheitsfunktionen der Appliance nutzlos. Die richtige Konfiguration der Features setzt darüber hinaus Expertise voraus und ist ebenso zeitaufwendig wie die notwendigen Anpassungen und Zertifikatsaktualisierungen.

4. Die neuesten Sicherheitsinformationen fehlen: KMU stehen schon lange im Fokus von Cyberkriminellen, und bereits 2019 tauchten pro Tag 312.000 neue Malware-Varianten im Netz auf, schreibt das Bundeskriminalamt in seinem „Cybercrime Bundeslagebild 2019". Angesichts dieser Sicherheitsbedrohung setzten Service Provider Cloud-basierte Gateways ein, um zu gewährleisten, daß ihre Kunden durch aktuelle Definitionen geschützt sind. Auf lokalen UTM-Geräten werden die veröffentlichten Definitionsdateien jedoch nur unregelmäßig heruntergeladen. Das öffnet neuen Varianten von Malware die Tür, unbemerkt ins Firmennetzwerk einzudringen.

5. Mehrkosten für Basics: Die Leistung der Appliance nimmt ohne zusätzliche Investitionen im Laufe der Zeit ab. Um zum Beispiel die verfügbare Bandbreite für ein höheres Datenaufkommen, neue Mitarbeiter oder andere Standorte hinzuzufügen, wird ein kostenpflichtiges Upgrade fällig. Zweigstellen verlangen entweder ein weitere Appliance oder teure MPLS-(Multiprotocol Label Switching)-Standverbindungen, um den Datenverkehr über die Zentrale zu leiten. Die Geräte selbst benötigen IT-Experten vor Ort, um sie einzurichten und regelmäßig sicherheitsrelevante Upgrades durchzuführen. Unterm Strich summieren sich die unverzichtbaren Mehrausgaben für die UTM-Lösung schnell.

Die Cloud-Alternative steht bereit: Bei komplexen Bedrohungen, flexiblen Arbeitsmodellen sowie zunehmendem Cloud-Einsatz bleiben UTM-Appliances weitgehend wirkungslos. Genau den Sicherheitsbedarf von KMU adressiert ein Software-definiertes Sicherheitsmodell (SDSec) aus der Cloud, das ein Security Web Gateway und eine Sicherheitsplattform kombiniert. Das Gateway blockiert suspekte Downloads und als bösartig bekannte Websites. Die Cloud-Plattform umfaßt Sicherheitsdienste für Endgeräte, Netzwerke und Datensicherung und stellt eine zentrale Konsole zur Geräte- und Richtlinienverwaltung, Report-Funktionen sowie Sicherheitswarnungen in Echtzeit bereit. Anwenderfirmen erhalten so eine Cloud-basierte Lösung, die stets auf dem aktuellen Patch-Stand ist, Sicherheitslücken schließt und die Sicherheit auf dem Niveau von Großunternehmen bietet – bei Bedarf auch als Managed Service.