© Wortmann AG

Sicherheit zum Dazwischenschalten

Eine Firmenpackung Abwehrkräfte

IT-Sicherheit ist komplex. Die Bedrohungen kommen in nahezu unendlicher Vielfalt daher. Dagegen steht ein fast ebenso unüberschaubares Arsenal von Lösungen. Kein Wunder, dass mancher Verantwortliche lieber den Kopf in den Sand steckt. Dabei können auch kleine Unternehmen für wenig Geld zu umfassendem Schutz kommen.

Von Uli Ries

Kein Unternehmen darf sich heute mehr ohne Absicherung der IT-Infrastruktur ins Netz trauen. Nur kann eine umfangreiche Sicherheitsinfrastruktur aus Firewall, Intrusion Detection System, Virenscannern, Spam-Filter, VPN-Gateway und Proxy-Server schnell Dimensionen von mehreren zehntausend Euro erreichen.

Das ist eindeutig zu viel für kleine oder mittelständische Unternehmen. Und nur allzu oft auch überdimensioniert. Von einer überschaubaren IT-Mannschaft ist das gar nicht sinnvoll zu administrieren und zu betreiben.

Kleinere Organisationen sind dennoch nicht dazu verdammt, sich mit lokal auf den PCs installierten Virenscannern und Desktop-Firewalls zufriedenzugeben. Denn mit so genannten UTM-Appliances (Unified Threat Management) haben die Hersteller von IT-Sicherheitsprodukten eine Produktkategorie geschaffen, die kleinere Netze wirksam absichert, gleichzeitig aber keine Löcher in die IT-Budgets reißt. Schon ab 200 Euro sind UTM-Appliances zu bekommen.

Faustdicke Funktionen

Je nach Hersteller unterscheidet sich der Leistungsumfang der Appliances. Die im Übrigen nicht immer ein Stück Hardware sein müssen. Manche

UTM-Produkte gibt es bei gleichen Funktionen auch als Software, die je nach Ausbaustufe und Anforderung sogar in einer virtuellen Maschine laufen kann.

Kommt es auf möglichst hohen Datendurchsatz an, verbietet sich eine solche Konstruktion natürlich. Dann hilft nur eine eigenständige Hardware.

Bei allen Unterschieden sind folgende Funktionen allen UTM-Lösungen gemeinsam: Firewall, Spam-Filter, Antivirenlösung und Intrusion Detection System. Dazu kommen zumeist noch VPN-Funktionen und Inhaltsfilter, um z.B. im Webdatenstrom nach bestimmten Stichworten zu fahnden. Manche Hersteller packen auch noch eine Funktion zum Untersuchen von per SSL verschlüsselten Datenströmen in ihre Produkte oder bieten die Möglichkeit, VoIP-Telefonate abzusichern.

Der Vorteil einer solchen Komplettlösung: Sparsame Kunden müssen nicht auf eine essenzielle Komponente verzichten, sondern bekommen in jedem Fall einen Rundumschutz.

Viel Schutz, wenig Mühe

Egal, ob die unternehmenseigene IT-Mannschaft die UTM-Appliance betreut oder ob das von einem Systemhaus übernommen wird, ein Vorteil kommt allen zugute: Sämtliche Schutzfunktionen lassen sich über ein einheitliches Interface administrieren. Kämen eigenständige Schutzprodukte zum Einsatz, brächte jedes seine eigene Benutzeroberfläche mit. Der Aufwand wäre erheblich höher, die Wahrscheinlichkeit wäre größer, dass man einen wichtigen Hinweis in einer Logdatei übersieht.

In der Praxis empfiehlt es sich, die UTM nicht nur von einem Systemhaus installieren zu lassen. Auch der laufende Betrieb und das dazu gehörende Auswerten der Logfiles ist bei Spezialisten meist in besseren Händen. Denn es ist ein weit verbreiteter Irrglaube, dass eine solche Appliance lediglich zu Anfang konfiguriert werden muss und von da an ihren Dienst im Serverraum verrichtet. Ohne regelmäßige Prüfung der Protokolle ist einem subtilen Angriff kaum auf die Schliche zu kommen.

Auch die Erstkonfiguration will mit Bedacht und Sachverstand erledigt werden. So gilt es u.a. zu klären, welche PCs bzw. Anwender auf welche Internet-Dienste zugreifen dürfen. UTM-Appliances erlauben solche Einschränkungen meist per White-/Blacklist. Kommen im Lauf der Zeit Mitarbeiter hinzu oder ändern sich die Aufgaben, müssen diese Einstellungen in der UTM-Lösung angepasst werden. All dies sind Tätigkeiten, die ein spezialisiertes Systemhaus effizient erledigt.

Einsatz im Realbeispiel

Am besten zeigt die Erfahrung, in welchen Szenarien Systemhäuser mit UTM-Lösungen erfolgreich für Sicherheit gesorgt haben: IT for Life aus Jübek konnte z.B. über 70 Zahnarztpraxen von einem Schutz per UTM überzeugen. Der Grund: Dank einer UTM-Appliance laufen die PCs in den Praxen zu ungeahnten Höchstleistungen auf. Und Performance ist das A und O, wo Röntgenaufnahmen digital erzeugt und sofort am PC anzeigt werden sollen. Das Verarbeiten der großen Bilder fordert die PCs erheblich. Ist auf diesen Computern noch ein lokaler Virenscanner installiert, dauert der Bildaufbau unakzeptabel lange.

Die Lösung: IT for Life entfernte die Virenscanner, setzte eine UTM-Appliance ein und verbot den betreffenden, weitgehend schutzlosen PCs den Internet-Zugriff. Außerdem sperrte man alle Schnittstellen wie USB-Ports, um das Einschleppen von Malware per USB-Stick oder MP3-Player zu verhindern. Durch diese strikte Reglementierung kommen die PCs nun nicht mehr ins Schwitzen, teure Neuhardware entfällt. Unterm Strich war die UTM-Appliance inklusive Installation und vorheriger Konfigurationsplanung erheblich günstiger als ein Schwung neuer PCs.

Andere Rechner im Praxisnetzwerk, bei denen die Leistung weniger kritisch ist, haben natürlich Internet-Zugang und funktionierende USB-Schnittstellen. Auf diesen Maschinen arbeitet dann auch ein lokaler Virenscanner. Denn es kommt im Praxisalltag oft vor, dass Patienten ihre Röntgenbilder oder andere Patienteninformationen auf einem USB-Stick mitbringen. Auf diese Weise könnte sich leicht Malware auf den vernetzten PCs der Praxis breit machen.

Ein so radikaler Schritt, wie ihn das Systemhaus IT for Life im Fall der Zahnärzte geht, ist sicher nicht die Norm. In aller Regel dürften lokale Virenscanner auf sämtlichen Clients die Schutzfunktionen der UTM-Appliance ergänzen. Das ist auch dringend zu empfehlen und wird von IT for Life auch so umgesetzt, da die Firewall in Verbindung mit dem integrierten Malware-Scanner sicher nicht alle Schädlinge aus dem Datenstrom fischt.

Kontrolle mit kurzer Leine

Auch bei WB IT-Systeme in Laatzen hat man die Erfahrung gemacht, dass Unternehmen ab fünf mit dem Internet verbundenen PC-Arbeitsplätzen perfekt mit einer UTM-Appliance bedient werden. Neben dem üblichen Schutz gegen Schadsoft-

© Securepoint

Securepoints UTM-Appliances gibt es in diversen Ausführungen, darunter auch eine reine Softwarelösung.

ware und Spam wünschen viele Kunden auch einen Schutz gegen (unbeabsichtigte) Angriffe von innen: Ganz oben auf der Wunschliste steht die Funktion, den Internet-Zugang zu reglementieren.

Damit wollen sich die Auftraggeber u.a. rechtliche Probleme ersparen, die aus eventuell fragwürdigen Aktivitäten der Mitarbeiter resultieren können. Gleichzeitig minimiert man so natürlich auch die Gefahr, dass die PCs Opfer einer Attacke werden, die von einer bösartig modifizierten Internet-Seite ausgeht. Verstöße gegen firmeninterne Regelungen lassen sich anhand der integrierten Nutzerauthentifizierung genau nachvollziehen.

Alleskönner oder Spezialisten?

So smart die Kombination verschiedener Schutzfunktionen in einem Gerät auch ist – eigenständige Lösungen sind in der Regel leistungsfähiger. Eine dedizierte Firewall wird normalerweise deutlich mehr können als die in eine UTM-Appliance integrierte. Das Gleiche gilt für den Malware-Schutz. Einzelne Schutzprodukte erledigen überdies auch spezielle Aufgaben wie das Absichern von Datenbanken oder von bestimmten Web-Anwendungen. Herkömmliche Firewalls – zu denen auch die in den UTM-Appliances gehören – können den an solche Anwendungen gerichteten Datenverkehr nicht von üblichem Webtraffic unterscheiden und erkennen daher auch keine Auffälligkeiten.

Leistungsfähiger sind eigenständige Systeme auch beim Auswerten der Netzwerkaktivitäten. Umfangreiche Filter zum zielsicheren Durchsuchen des Wustes aus TCP/IP-Ports, Internet-Protokollen, Uhrzeiten, Datenstromrichtungen und anderen Angaben helfen dem Administrator. Fehlen sie, wird das Auswerten zum Geduldsspiel.

An seine Grenzen gerät Unified Threat Management auch, wenn das Netzwerk eine gewisse Größe überschreitet bzw. die Netzwerkbandbreite stark anschwillt. Dann sind getrennte Systeme leistungsfähiger, da hier jedes nur eine Aufgabe übernimmt. Als Faustregel gilt: Ab 500 Webnutzern sollten dezidierte Schutzmechanismen ins Auge gefasst werden. Andernfalls droht die UTM-Lösung zum Flaschenhals zu werden.

Als dynamisches Duo

Hinzu kommt die Tatsache, dass UTM-Produkte konzeptbedingt so genannte Single Points of Failure sind. Das bedeutet: Wenn eine einzelne Komponente ausfällt, stehen alle Räder still. In diesem Fall würde der Ausfall der UTM-Appliance bedeuten, dass keinerlei Internet-Konnektivität mehr geboten ist. Bei eigenständigen Komponenten bedeutet z.B. der Absturz der Antivirensoftware noch lange keine Online-Zwangspause.

Zumindest dieses Problem lässt sich im UTM-Umfeld aber einigermaßen elegant lösen: Hersteller wie Securepoint geben ihren Produkten von Haus aus die Fähigkeit zur Redundanz mit auf den Weg. Je nachdem, wie kritisch die Appliance ist, kann der Kunde sich entscheiden: Entweder er wählt die günstige Option des Cold Standby, oder er entscheidet sich für das teurere Hot Standby. Bei Letzterem laufen zwei UTM-Appliances ständig im Parallelbetrieb, wobei nur eine tatsächlich aktiv ist. Die zweite übernimmt zwar augenblicklich sämtliche Konfigurationsänderungen der ersten und versorgt sich auch permanent mit allen Antivirenupdates aus dem Internet. Aktiv wird die Ersatz-Appliance allerdings erst, wenn die Haupt-UTM-Lösung aus irgendeinem Grund nicht mehr funktionstüchtig ist. Der Nachteil: Der Kunde muss für die Standby-Appliance mindestens das Lizenzgrundpaket (fünf Lizenzen) kaufen.

Quasi gratis, aber trotzdem hinreichend sicher ist das Cold-Standby-Konzept. Securepoint erlaubt

jedem Kunden, eine zweite Appliance zu installieren und diese nach Belieben von Hand mit den Konfigurationsänderungen und Virensignaturdateien zu versorgen. Fällt eine UTM aus, muss man die zweite manuell in den Live-Betrieb versetzen. Jörg Hohmann, Director für Sales und Marketing bei Securepoint, erklärt, dass das Umschalten auf die Ersatz-UTM normalerweise binnen weniger Minuten über die Bühne geht – vorausgesetzt, die Appliance kennt die aktuelle Konfiguration und ist auf aktuellem Stand.

Attraktiv in Preis und Leistung

Wie bereits erwähnt, finden UTM-Appliances zumeist dank ihrer niedrigen Anschaffungskosten den Weg in kleinere und mittelgroße Unternehmen. Natürlich gibt es auch UTM-Appliances im Gegenwert einer Zwei-Zimmer-Eigentumswohnung in Metropolenlage. Für kleinere Unternehmen kommt so etwas aber kaum in Frage.

Durchweg hohe Akzeptanz finden die Modelle des deutschen UTM-Herstellers Securepoint. Mit Einstiegspreisen von 299 Euro bekommen auch kleine Unternehmen eine Appliance, die einen soliden Basisschutz verspricht.

Securepoint-Vertriebsmann Jörg Hohmann sieht die Produkte vor allem in IT-Umgebungen, die zwischen fünf und 250 IT-Arbeitsplätze umfassen. Seiner Auskunft nach finden insbesondere vergleichsweise kleine Unternehmen wie Arztpraxen, Steuerberatungs- oder Anwaltskanzleien kaum geeignete – lies: bezahlbare – Angebote beim Mitbewerb. Da aber gerade diese Klientel nicht zuletzt per Gesetz zu striktem Datenschutz gezwungen ist, tun Schutzmaßnahmen Not.

Als großen Vorteil der Securepoint-UTM-Lösungen sieht Hohmann das bündige Preiskonzept: Kunden bezahlen nur die Anzahl der gewünschten Lizenzen. Es fallen keine weiteren Kosten für zusätzliche Schutzfunktionen an, alle Mechanismen der Appliances stehen uneingeschränkt zur Verfügung. Dazu gehört auch ein sich stündlich aktualisierender Virenschutz.

Securepoint setzt hier auf die in der Unix-Welt beliebte Scan-Engine ClamAV. Der Spam-Filter stammt von der israelischen Firma Commtouch. Besonders stolz ist Hohmann auf das Service- und Supportkonzept: Da alle Produkte in Deutschland entwickelt werden, kann Securepoint jederzeit und im Handumdrehen eventuell auftauchende Probleme lösen. Sprachbarrieren und unterschiedliche Zeitzonen spielen keine Rolle. Jeder Securepoint-Partner – in aller Regel Systemhäuser, das Direktgeschäft spielt für Securepoint so gut wie keine Rolle – bekommt uneingeschränkten, kostenfreien Support.

Wachsam bleiben und gewinnen

Mit Unified Threat Management können Kunden auf einen leistungsfähigen Rundumschutz vertrauen, während Systemhäuser mit überzeugenden Argumenten ihren Absatz steigern. Schließt der Kunde einen Servicevertrag, profitieren wiederum beide Seiten. Zum einen genießen die Kunden so kontrollierten Schutz, zum anderen kann sich das Systemhaus regelmäßiger Umsätze sicher sein.

Eines sollten beide Seiten aber niemals vergessen: Vollständige Sicherheit gibt es nicht. Keine noch so ausgefuchste UTM-Appliance und kein noch so schlagkräftiger Verbund aus Sicherheitsprodukten wehrt sämtliche Cyber-Attacken ab.

Es gilt daher, stets wachsam zu bleiben. Anwender müssen mögliche Gefahren erkennen können, Unternehmensverantwortliche müssen klare Regeln aufstellen, was im Netz und beim Umgang mit Unternehmensdaten erlaubt ist. Und Systemhäuser sollten jederzeit darauf gefasst sein, in den Logdateien ihrer Kunden Merkwürdigkeiten zu entdecken. Denn vielleicht ist ja der eigene Kunde ins Visier der Cyber-Gangster geraten?

Das per Webbrowser zugängliche Securepoint-Cockpit zeigt auf einen Blick alles Wissenswerte über den Zustand der UTM-Appliance.