# IT-Journal

Ausgabe 2/2015

## In dieser Ausgabe

**End-To-End Security** S. 1
Fortinet

**Editorial** S. 2
Wissen Sie wie sicher Ihre IT ist?

**IT-Security** S. 3
Welche Arten von Bredohungen gibt es?

**IT-Security** S.4
Welche Anforderungen haben Sie an Ihre IT-Umgebung?

**IT-Security** S.5
FortiAuthenticator Appliance

**Deep Security** S.6/7
Trend Micro

**Neuigkeiten von BASYS** S.8
Veranstaltungen von BASYS
Aus-und Rückblick

# END-TO-END SECURITY

### FortiGate - Next Generation Firewalling (NGFW) und Unified Threat Management (UTM)

Fortinet bietet mit der Produktfamilie „FortiGate“ eine ganze Palette von mehrfach ausgezeichneten Appliances für den Schutz von Netzwerken und Applikationen. Die FortiGate Systeme schützen Daten zuverlässig und in Echtzeit vor Netzwerk- und Content-basierenden Bedrohungen.

Hier spielen die von Fortinet entwickelten ASIC Prozessoren eine entscheidende Rolle, welche die vielfältigen Dienste und Sicherheitsfunktionen der FortiGate-Appliances enorm beschleunigen. Somit lassen sich Bedrohungen durch Viren, Würmer, Exploits, Spyware oder neuartigen sog. Blended Threats, also Kombinationen aus den vorgenannten Angriffsmustern, effektiv bekämpfen - und das in Echtzeit!
Weitere Funktionen wie umfangreiche und komfortable Applikationskontrolle, URL-Filter, IPSec- und SSL-VPN, Bandbreitenmanagement, WLAN-Controller, integrierte 2-Faktor-Authentifizierung und selbstverständlich eine marktführende Firewall sind fest integrierter Bestandteil aller FortiGate Appliances.
Bedrohungsszenarien richten sich nicht nach Unternehmensgrößen, und so bieten alle FortiGate Appliances nahezu denselben Funktionsumfang und dieselbe Bedienung per grafischer Oberfläche oder CLI (command line Interface).

Die User-unabhängige Lizenzierung aller Module vereinfacht das Netzwerk-Design, ermöglicht Kosten transparenz und den flexiblen Einsatz der Produkte.
Auch kleinere Unternehmen profitieren so von Fortinets Erfahrung aus Großprojekten und können so bei sehr gutem Preis-Leistungsverhältnis mit einem hervorragenden Schutz bei außergewöhnlicher Flexibilität Ihre Netzwerke und Daten absichern.

BASYS EDV-SYSTEME

# Editorial

**Die meisten Geschäftsprozesse sind vom verlässlichen und fehlerfreien Funktionieren der IT-Systeme abhängig. Ratingagenturen bewerten die Sicherheit der IT als Teil der operationellen Risiken eines Unternehmens.**

Die in Unternehmen verbreitete Einstellung „Bisher ist nichts passiert" kann zu ernsthaften Problemen führen, wenn bestehende Sicherheitskonzepte nicht kontinuierlich und angemessen an die variierende Bedrohungslage angepasst werden.

Unabhängig davon nimmt die Anzahl der Bedrohungen auch stetig zu, weshalb die Wahrscheinlichkeit, dass ein Unternehmen oder eine Behörde von einem Cyber-Angriff betroffen ist, rasant ansteigt. Je nach Abhängigkeit von der IT kann die Unternehmenstätigkeit komplett zum Stillstand gebracht werden – mit allen Konsequenzen, die damit verbunden sind.

**IT- Sicherheit sollte daher Chefsache sein.**

Wir möchten gerne im Folgenden erläutern, warum dies so ist und welche Lösungen es gibt, um die unterschiedlichen Anforderungen an die IT-Sicherheit zu erfüllen. Im Einzelnen beschäftigen wir uns mit den Fragen:

- Welche Arten von Bedrohungen gibt es?
- Welche Security Anforderungen werden an eine IT-Umgebung gestellt?
- Welche Lösungen gibt es um die Sicherheit eines IT-Systems zu gewährleisten?
- Wie kann die Sicherheit eines IT-Systems überprüft und kontinuierlich sichergestellt werden?

Ich wünsche Ihnen viel Spaß beim Lesen.

Ihr Stephan Michaelsen

# Wissen Sie wie sicher Ihre IT ist?

**Warum ist IT-Security ein so wichtiges Thema?**

Die aktuelle Gefährdungslage für die IT bleibt hinsichtlich des zu verzeichnenden Angriffspotenzials kritisch. Nicht nur die Anzahl schwerer Sicherheitslücken in den meistverbreiteten IT-Systemen rangierten auf sehr hohem Niveau. Auch die Werkzeuge zur Ausnutzung dieser Verwundbarkeiten stehen einer immer größer werdenden Anzahl an Angreifern zur Verfügung, die diese aus der Anonymität des globalen Cyber-Raums für ihre Zwecke einzusetzen bereit sind.

**Die Herausforderungen für die IT-Security:**

**1. Technologische Durchdringung und Vernetzung:**
Alle physischen Systeme werden von IT erfasst und schrittweise mit dem Internet verbunden.

**2. Komplexität:**
Die Komplexität der IT nimmt durch vertikale und horizontale Integration in die Wertschöpfungsprozesse erheblich zu.

**3. Allgegenwärtigkeit:**
Jedes System ist praktisch zu jeder Zeit und von jedem Ort über das Internet erreichbar.

Als Folge der schnell voranschreitenden Digitalisierung und Vernetzung ergibt sich, dass der Schutz der IT-Netze und IT-Systeme an den Außengrenzen des Unternehmens immer weiter erodiert und sich neue Angriffsflächen eröffnen. Auch werden IT-Systeme angreifbar, die bislang aus dem Internet gar nicht erreichbar waren. Mit steigender Komplexität der Systeme stoßen altbekannte konventionelle IT-Sicherheitsmechanismen schnell an ihre Grenzen und vermögen es nicht, Zuverlässigkeit und Beherrschbarkeit im gewohnten Maße zu gewährleisten.

Wer sich umfassend zu diesem Thema informieren möchte, dem empfehlen wir den Bericht "Die Lage der IT-Sicherheit in Deutschland 2014" zu lesen. Diesen hat das Bundesamt für IT-Sicherheit in der


Informationstechnik Ende 2014 herausgegeben. Darin wird verständlich beschrieben, welche Bedrohungen es gibt, welche Auswirkungen diese haben und wie sich Unternehmen schützen können.

Alleine diese ersten Aufzählungen verdeutlicht, wie komplex das Thema IT-Sicherheit mittlerweile geworden ist und wie aufwendig es ist die Sicherheit eines IT-Systems zu gewährleisten.

BASYS arbeitet unter anderem mit folgenden Herstellern im Bereich IT-Security zusammen:

FORTINET
TREND MICRO
enQsig E-Mail. Vertraulich.
Net at Work
arcserve
Microsoft

# Welche Arten von Bedrohungen gibt es? Was sind Cyber- Angriffe?

**Cyber-Angriffe werden sowohl in der Breite als auch zielgerichtet gegen Einzelpersonen oder Institutionen eingesetzt. Die nachfolgende Aufzählung gibt einen Überblick über die heute genutzten Angriffsmethoden.**

**Spam**
Dies sind unerwünschte Nachrichten, die massenhaft und ungezielt versendet werden. In der harmlosen Variante enthalten sie meist nur unerwünschte Werbung. Häufig enthalten Sie aber auch Schadprogramme im Anhang oder über Links zu Web-Seiten. Für den Versand von Spam-Nachrichten sind umfangreiche Ressourcen wie Botnetze oder kompromittierte Server notwendig.

**Schadprogramme**
Hierbei handelt es sich um Werkzeuge, mit deren Hilfe ein Angreifer Kontrolle über ein infiziertes System ausüben kann. Es gibt eine Reihe von unterschiedlichen Typen von Schadprogrammen, wie z.B. Viren, Trojaner, Bots oder Rootkits.
Die Gesamtzahl der PC-basierten Schadprogrammvarianten übersteigt Schätzungen zufolge bereits die 250 Millionen Marke.

**Drive-by-Exploits und Exploit-Kits**
Damit wird die automatisierte Ausnutzung von Sicherheitslücken durch das Aufrufen von präparierten Webseiten bezeichnet. Ohne Benutzerinteraktion werden dabei Schwachstellen im Browser, in Plug-ins oder im Betriebssystem ausgenutzt, um unbemerkt Schadprogramme auf dem System zu platzieren. Exploit-Kits spielen eine zentrale Rolle bei Cyber-Angriffen mit kriminellem Hintergrund.

**Botnetze**
Sind ein Verbund von Systemen, die von einer fernsteuerbaren Schadprogrammvariante (einem sogenannten Bot) befallen sind. Die infizierten Systeme werden vom Botnetz-Betreiber mittels eines Command- and Control-Servers gesteuert. Kriminelle nutzen Botnetze um im großen Stil Identitätsdiebstahl zu begehen, Angriffe auf die Verfügbarkeit von Computer-Systemen durchzuführen (DDoS-Angriffe) oder um massenhaft Spam bzw. Phishing-Mails zu versenden.

**Social Engineering**
Beim Social Engineering versuchen die Angreifer Ihre Opfer dazu zu verleiten, eigenständig Daten preiszugeben, Schutzmaßnahmen zu umgehen oder eigenständig Schadsoftware zu installieren. Die Cyber-Kriminellen gehen dabei geschickt vor um menschliches Verhalten wie Neugierde, Hilfsbereitschaft und auch Naivität auszunutzen. Häufig ist Social Engineering ein elementarer Bestandteil von gezielten Angriffen.

**Identitätsdiebstahl oder Identitätsmissbrauch**
Damit wird die Aneignung und unberechtigte Verwendung personenbezogener Daten durch Dritte bezeichnet. Das Ziel des Angreifers ist es, in der Regel finanzielle Vorteile zu erlangen oder in den Besitz vertraulicher Informationen zu gelangen. Ein Angriff auf eBay im Mai 2014 betraf beispielsweise weltweit 145 Millionen Kunden, davon alleine ca. 15 Millionen in Deutschland.

**Denial of Service**
Diese Angriffe richten sich gegen die Verfügbarkeit von Diensten, einzelnen Systemen oder ganzen Netzen. Häufig wird ein solcher Angriff von vielen Systemen parallel ausgeführt. Man spricht dann von einem DDoS-Angriff (DDoS = Distributed Denial of Service). Diese Angriffe erfolgen meistens gegen große Unternehmen, Regierungen und E-Commerce-Anbieter. Immer häufiger sind aber auch Betreiber Kritischer Infrastrukturen (KRITIS) betroffen.

**Advanced Persistent Threats (APT)**
Hierbei handelt es sich um sehr zielgerichtete Angriffe auf spezifisch ausgewählte Institutionen und Einrichtungen. Die Angriffe zeichnen sich in der Regel durch einen hohen Ressourceneinsatz und erhebliche technische Fähigkeiten aus und sind meistens nur schwierig zu detektieren. APT-Angriffe sind eine ernste Bedrohung für die Wirtschaft und die öffentliche Verwaltung. Das Hacking von schlecht gesicherten Unternehmensnetzen wird künftig weiter an Bedeutung zunehmen.

**Nachrichtendienstliche Cyber-Angriffe**
Besonders durch die Enthüllungen von Edward Snowden ist auch einer breiten Öffentlichkeit bewusst geworden, in welchen Ausmaß und mit welchen gigantischem Aufwand die Nach-richtendienste Cyber-Angriffe durchführen und Informationen ausspähen.

# Welche IT-Security Anforderungen haben Sie an Ihre IT-Umgebung?

**Als Folge der schnell voranschreitenden Digitalisierung und Vernetzung unserer Welt und der stetig steigenden Komplexität der eingesetzten IT-Systeme ergeben sich immer neue Anforderungen an die IT-Sicherheit. Was erwarten Sie?**

Anhand von einfachen Aussagen bzw. Anforderungen möchten wir Ihnen im Folgenden aufzeigen, welche verschiedenen Systeme und Lösungen zum Einsatz kommen sollten, um die Sicherheit Ihrer IT-Systeme zu gewährleisten.

Wenn einige oder sogar alle Aussagen auf Sie zutreffen und Sie wissen möchten, welche Kombination der verschiedenen Systeme für Ihre IT-Umgebung die optimale Lösung darstellt, sprechen Sie uns an und vereinbaren Sie einen Termin mit einem unserer IT-Security Experten.

Wie die aktuellen Beispiele aus Berlin zeigen, wer nicht rechtzeitig auf die Sicherheit seiner IT-Systeme achtet, muss ggf. mit einem sehr hohen Aufwand seine gesamten Systeme neu aufsetzen.

Meine IT-Umgebung soll vor unbefugten Zugriffen von außen geschützt werden.
Die Lösung: **Firewall-Systeme**

Ich möchte den Zugriff auf mein internes Netzwerk nur bestimmten / bekannten Geräten erlauben.
Die Lösung: **Network Access Control (NAC)**

Meine Daten sollen nur von befugten Personen gelesen werden können.
Die Lösung: **Verschlüsselung**

Ich möchte die "Echtheit" der Identität von Personen und Geräten überprüfen, die auf mein IT-System zugreifen wollen.
Die Lösung: **Authentifizierung**

Ich will Personen und Geräten, deren Identität ich überprüft habe, bestimmte Rechte zuweisen können, damit diese nur bestimmte, erlaubte Aktionen auf meinem IT-System ausführen können.
Die Lösung: **Autorisierung / Zugriffskontrolle**

Ich will Angriffsversuche auf mein Netzwerk erkennen und abwehren können.
Die Lösung: **Intrusion Detection / Intrusion Prevention Systeme (IDS/IPS)**

Ich will Schadsoftware erkennen, finden und ggf. löschen können.
Die Lösung: **Viren-/ Malware-Schutz**

Ich möchte den Zugriff auf und die Nutzung von bestimmten Seiten und Diensten im Internet erlauben und /oder verbieten.
Die Lösung: **Web- / URL-Filtering**

Ich will den Erhalt von unerwünschten Mails (Spam) in meinem Mail-System verhindern.
Die Lösung: **Spam-Schutz**

Ich will meine Standorte sicher über das Internet miteinander verbinden.
Die Lösung: **VPN**

Ich möchte, dass in meinem IT-System nur bestimmte, zugelassene Anwendungen ausgeführt werden dürfen.
Die Lösung: **Applikationskontrolle**

Ich will verhindern, dass bestimmte, sensible Daten mein IT-System verlassen (z.B. durch USB-Sticks, Mail-Versand, hochladen in die Cloud, über Chat-Foren, etc.).
Die Lösung: **Data Loss Prevention**

Ich möchte, dass meine installierten Software Produkte immer den aktuellsten Sicherheitsanforderungen entsprechen.
Die Lösung: **Patch-Management**

## Beispiele für Sicherheitslücken

**Hackerangriff auf den Bundestag:**
Trojaner im "Parlakom" Netzwerk-Sicherheitsexperten fanden bei der Untersuchung weitere "Beifänge", wie z.B. Malware mit schlecht gefäschsten Mails und empfehlen das komplette Netzwerk zu ersetzen.

**"LogJam"**
Sicherheitslücke bei verschlüsselten Verbindungen. Experten haben eine schwerwiegende Sicherheitslücke entdeckt, die Angreifern den Zugang zu verschlüsselten (HTTPS oder TLS/SSL) und damit vermeintlich sicheren Verbindungen zu Websites verschaffen kann.

**"Shellshock"**
Das ist eine sehr kritische Sicherheitslücke in der Kommandozeile (Bash), von Unix/Linux, auch Mac OS X ist davon betroffen.

**Kundendaten bei Ebay gestohlen**
Angreifern gelang es, millionenfach persönliche Daten und auch verschlüsselte Paswörter zu stehlen.

**"Dragonfly" – gezielte Angriffe auf Produktionsnetze:**
Mit dem 2014 bekannt gewordenen Schadprogramm Havex griff die sogenannte Dragonfly-Gruppe mehrere Dutzend deutsche Unternehmen an.

**"Heartbleed"**
Der Heartbleed-Fehler im Verschlüsselungsprotokoll SSL wird von IT-Experten als einer der schwerwiegendsten Sicherheitslücken der letzten Jahre bezeichnet.

**Support Ende von Windows XP**
Der Marktanteil von XP liegt im März 2015 bei knapp 17 Prozent, die Windows-Version 8 bzw. 8.1 landet, was die Nutzerzahlen angeht, auf einem Marktanteil von rund 14 Prozent. Microsoft beendete aber den Support für XP bereits am 8.4.2014.

# FortiAuthenticator Appliance

**Mit der FortiAuthenticator Appliance bietet Fortinet eine zentrale Instanz für „User Identity Management“ und „User Access Control“ an. Es werden unter anderem die Funktionen 2-Faktor-Authentifizierung, Identitätsverifikation und Netzwerkzugriffskontrolle (NAC) unterstützt.**

**Das Problem kennt jeder: Passwörter. Entweder sind sie gut, aber man kann sie sich nicht merken oder sie sind schlecht, weil es zu bequem ist, sich mit Guten abzuplagen.**

Häufig werden nach wie vor nur User-Name und Passwort als Authentifizierungs- und Autorisierungsmechanismen genutzt. Angesichts des laxen Umgangs mit diesen persönlichen Zugangsdaten ein äußerst unsicheres Verfahren.
Auch die Nutzung von komplexen Passwörtern löst dieses Problem nicht wirklich. Sie sind schwer zu merken und viele User verwenden deshalb die gleichen Passwörter für verschiedene Plattformen und Anwendungen. Wird eine Applikation gehackt, sind Angriffe auf die anderen Plattformen ein Kinderspiel.

### Zentrale Instanz für das User Identity Management

Eine sichere und zuverlässige User-Authentifizierung (Überprüfung der Echtheit der Person) und User-Autorisierung (Zuweisung von Rechten gemäß individueller Regeln) ist nur durch die Verwendung von intelligenten Login-Verfahren möglich.

Mit dem FortiAuthenticator stellt Fortinet hierfür eine richtungsweisende Plattform zur Verfügung.

FortiAuthenticator ist eine zentrale Instanz für die Zugriffssteuerung auf FortiGate-Appliances, auf Systeme von Drittanbietern, Websites und VPN-Zugänge. Unter anderem werden Funktionen wie 2-Faktor-Authentifizierung, Identitätsverifikation und Netzwerkzugriffskontrolle (NAC) bereitgestellt.

Dank der Unterstützung von LDAP und RADIUS, der nahtlosen Active Directory Einbindung, sowie der Integration von „Fortinet Single Sign On“ stehen diverse Funktionen zur Zugriffskontrolle der Benutzer zur Verfügung.

### 2-Faktor-Authentizierung mit unterschiedlichen Token

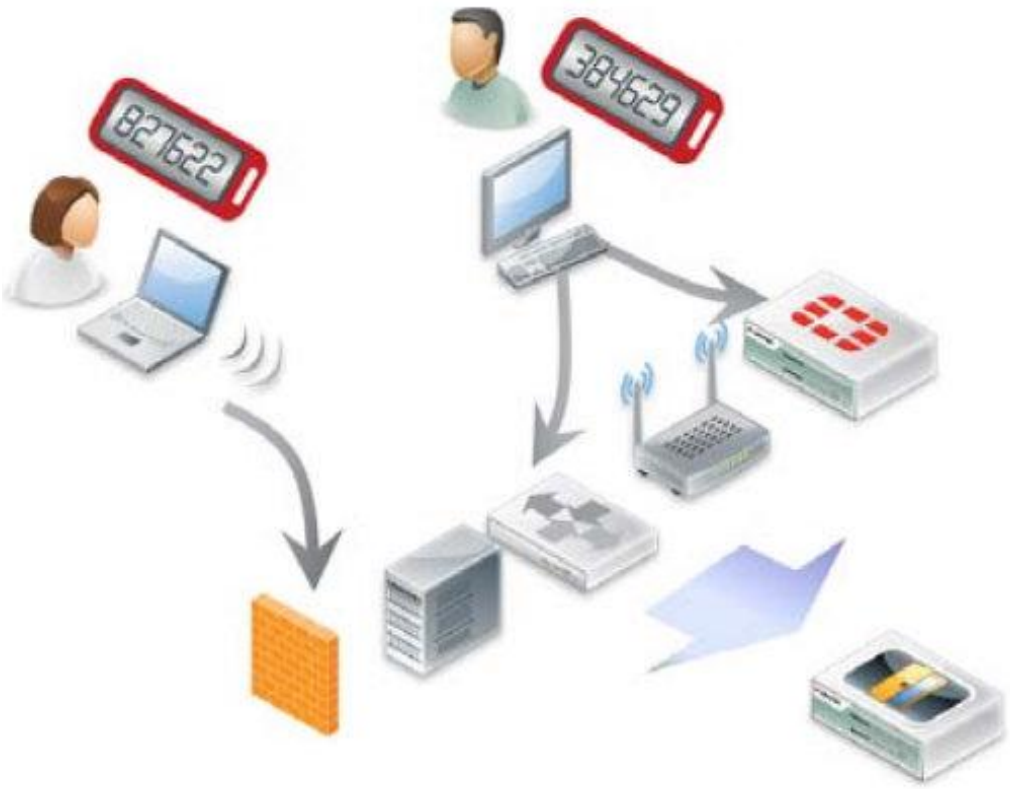
Durch die wahlweise Unterstützung von verschiedenen Token, die zeitbasierende Einmalpasswörter (OTP) generieren, kann der FortiAuthenticator in diversen Szenarien eingesetzt werden.

Neben der FortiToken Hardware können der FortiToken Mobile für unterschiedliche Smartphones sowie E-Mail und SMS Token genutzt werden.
Durch die Kombination aus Wissen (Zugangsdaten) und Besitz (Token) verhindern OTPs die Anmeldung von nicht autorisierten Personen und damit den unerlaubten Zugriff auf Netzwerk und Applikationen durch unbefugte Dritte. Zudem bilden sie, aufgrund des nur kurzzeitig gültigen Zugangscodes (max. 60 Sek.), einen wirksamen Schutz gegen Keylogger und ähnliche Attacken.

### FortiToken Mobile

Die App-basierende Clientsoftware FortiToken Mobile macht Smartphones und Tablets zu mobilen OTP-Token bzw. zum persönlichen Authentifizierungs-Device.

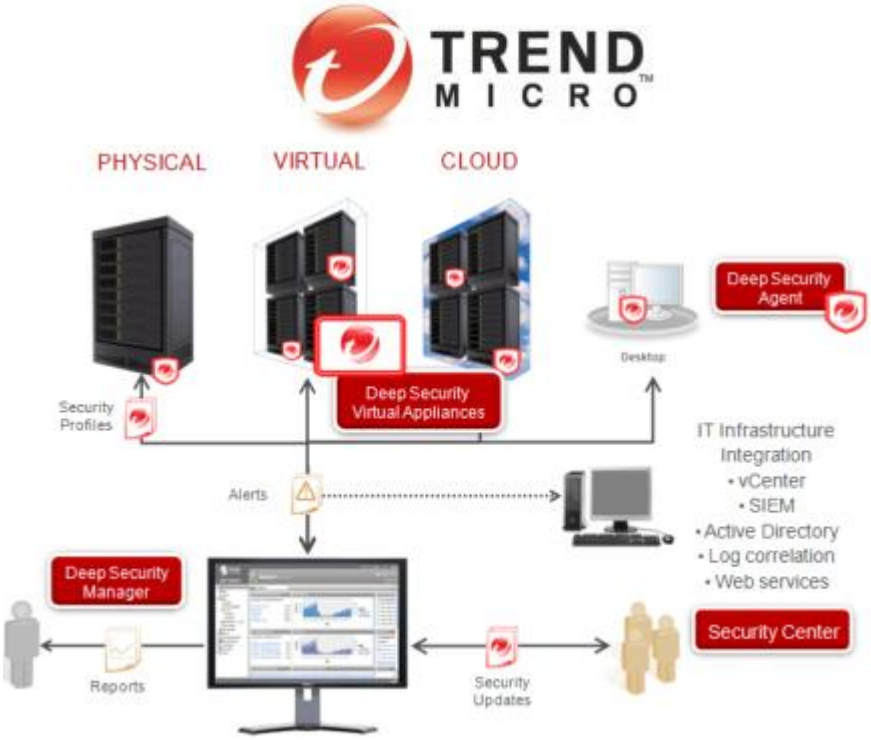
Gegenüber herkömmlichen Hardware -Token weist die Open-Authentication-(OATH-) konforme Lösung erhebliche Vorteile auf. Es wird keine weitere Hardware benötigt, das Rollout ist einfach und die Aktivierung der Token kann sehr komfortabel erfolgen.
Es werden sämtliche Benutzer-Authentifizierungsfunktionen wie VPN (SSL, IPsec), User-Administration und Captive-Portale durch den Software Token unterstützt.



# Trend Micro Deep Security

**Serversicherheit für Systeme, Anwendungen und Daten**

Zu den gefährlichsten IT-Security Ereignissen des Jahres 2014 zählen „Shellshock“ und „Heartbleed“. Bei genauer Be- trachtung stellt man fest, dass es sich nicht um klassische Viren oder sonstige Malware handelt, sondern es sind Schwachstellen, die schon seit geraumer Zeit in Bestands- systemen existierten und 2014 entdeckt wurden.
Anders als bei Viren und Trojanern, die an der Barriere eines Anti-Virenscanner vorbeugeschleust werden müssen, stan- den durch diese Sicherheitslücken die Türen zu den IT-Systemen weit offen.
In den meisten Unternehmen und Institutionen wird das Thema Viren- und Malware-Schutz bereits seit Jahren ziemlich vorbildlich behandelt. Innovative Techniken wie Intrusion Detection (Angriffserkennung) und Intrusion Prevention (Angriffsprävention), mit denen solche Lücken geschlossen werden können, kommen leider noch selten zum Einsatz.




### Intrusion Prevention / Intrusion Detection

Ein Intrusion Detection System (IDS) ist eine passive Komponente zur Abwehr von Angriffen, die anhand von abnormalem Netzwerkverkehr versucht Angriffsmuster zu erkennen. Ein Intrusion Prevention System (IPS) geht noch einen Schritt weiter. Ein IPS ist in der Lage bekannte Sicherheitslücken in einem System durch sogenanntes „virtuelles“ Patchen zu schließen. Dazu wird kein klassisches Patch-Management auf dem zu schützenden System betrieben, sondern es wird der schädliche Inhalt aus dem Datenstrom entfernt.
Dadurch ist es beispielsweise nicht mehr notwendig bei jeder Warnmeldung die Sicherheitsupdates für Java oder Flash einzuspielen. Das IPS schütz Ihre Systeme gegen Angriffe, obwohl nicht alle aktuellen Softwarepatche installiert sind. Auch solche Systeme, für die keine Sicherheitsupdates vom Hersteller mehr zur Verfügung gestellt werden (z.B. Windows XP), oder bei denen es wegen Abhängigkeiten zu anderen Programmen nicht möglich ist jeden Patch zu installieren, können auf diese Weise trotzdem zuverlässig vor Angriffen geschützt werden.

### Trend Micro Deep Security

Die Lösung Deep Security vom Hersteller Trend Micro bietet genau diese Möglichkeit. Durch das enthaltene Host-basierte IPS/IDS können sowohl physikalische wie auch virtuelle Systeme zuverlässig vor Angriffen geschützt werden.
In einer VMware vSphere Umgebung werden die virtuellen Maschinen agentenlos geschützt. Deep Security nutzt die in vSphere enthaltene Schnittstelle vShield Endpoint. Insbesondere für Umgebungen mit vielen virtuellen Maschinen (z.B. in einer VDI Umgebung) bietet dies erhebliche Performance-Vorteile, weil nicht mehr jede einzelne virtuelle Maschine die Sicherheitschecks durchführen muss. Für physikalische Systeme steht ein Agent bereit. Folgende Komponenten sind für das agentenlose Abwehren von Angriffsszenarien notwendig:

### Deep Security Manager

Die Administration der gesamten Lösung erfolgt zentral über die webbasierende Verwaltungskomponente Deep Security Manager. Darüber erfolgen alle Einstellungen, werden Scan-Policies definiert und auftretende Ereignisse erfasst.

### Deep Security Virtual Appliance

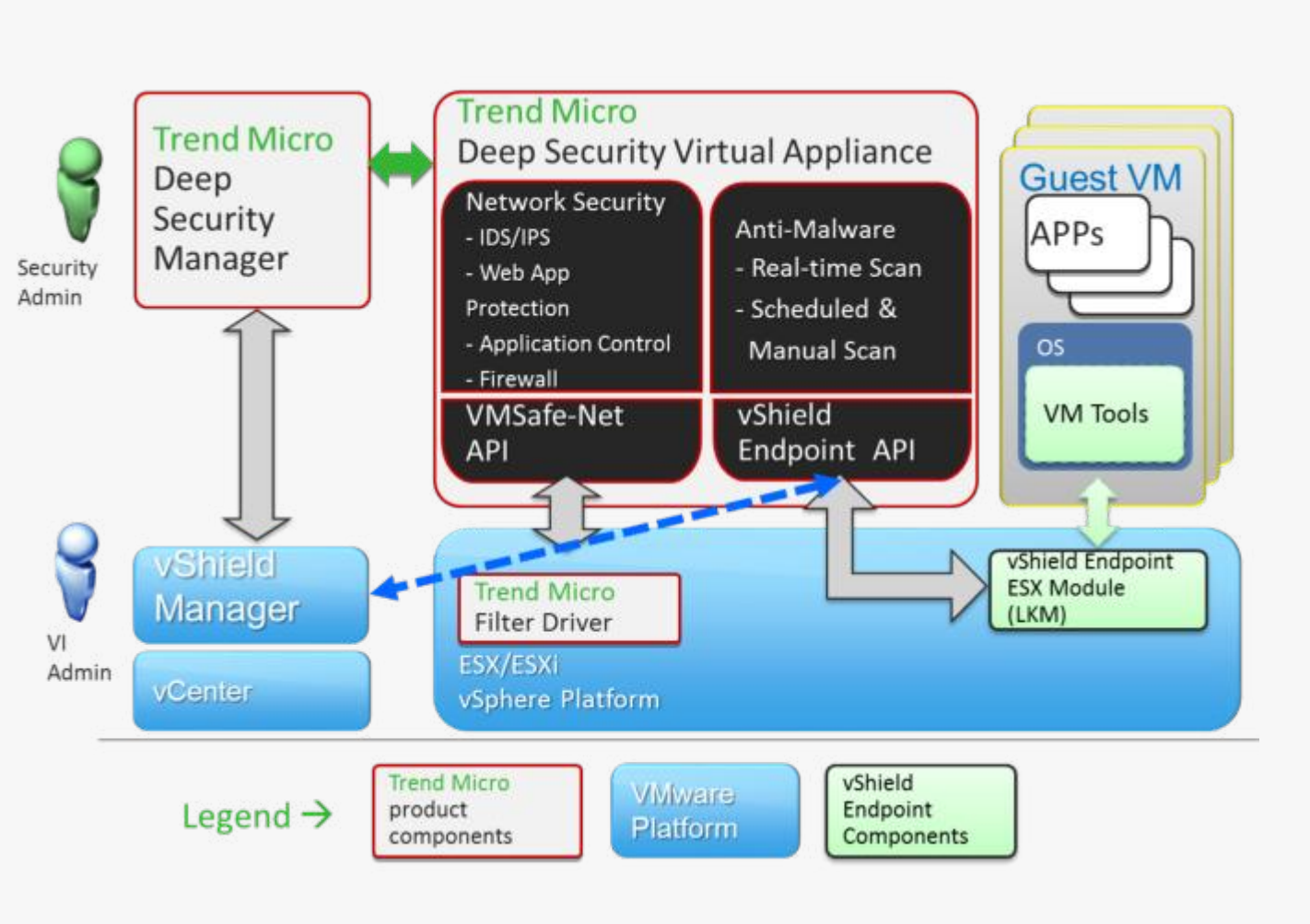
Die Deep Security Virtual Appliance wird auf jedem vSphere Host-System installiert und ist zuständig für die Umsetzung der im Manager festgelegten Policies und Sicherheits-mechanismen. Die Appliance übernimmt die Aufgabe des agentenlosen Malware-Scanning und insbesondere die Ab-wehr von Angriffsversuchen.

### VMware vShield Endpoint

Alle Module von Deep Security verwenden diese kostenfreie in jeder vSphere Lizenz enthaltene VMware Schnittstelle, für die Verbindung zu den virtuellen Maschinen.

### Filter Driver

Der Filter Driver, der auf jedem vSphere Host installiert wird, leitet den zu untersuchenden Datenverkehr an die Deep Security Virtual Appliance weiter. Dort wird der Inhalt der Datenpakete gegen bekannte Angriffsszenarien verglichen und bösartiger Verkehr entfernt.
In der folgenden Grafik ist das Zusammenspiel der Komponenten noch einmal bildlich dargestellt:




**Was ist normaler bzw. bösartiger Datenverkehr**
Eine der größten Herausforderungen bei der Einführung eines IPS/IDS Systems ist es festzulegen, welcher Datenverkehr als „böse" einzustufen ist. Um das Patchen aller Systeme umzusetzen, müssten die Versionen von allen Betriebssystemen und Anwendungen bekannt sein und diese müssten fortwährend gegen eine Datenbank mit den bekannten Sicherheitslücken (Vulnerabilities) abgeglichen werden. Dies ist eine wenig effiziente Methode für die Lösung dieser Aufgabenstellung.

Deep Security von Trend Micro bietet mit den Recommendation Scans eine wesentlich effizientere Vorgehensweise.

- Über die vShield Endpoint Schnittstelle wird von jedem virtuellen Zielsystem ein Paket an Informationen angefordert.
- Dieses Paket an Informationen, bestehend aus Versionsnummern, allgemeinen Systeminformationen, und Registry-Keys wird über die jeweilige Virtual Appliance auf dem Host an den Deep Security Manager weitergeleitet.
- Dort werden die Informationen gegen eine Datenbank mit bekannten Schwachstellen verglichen.
- Auf der Basis dieser Erkenntnisse können nun passende Policies für das untersuchte System generiert werden.
- Die Virtual Appliance übernimmt dieses Regelwerk wieder und kann das entsprechende Zielsystem so gegen Angriffsversuche und bösartigen Datenverkehr schützen.

Für virtuelle Windows-Systeme funktioniert dieser Vorgang komplett agentenlos. Unter Linux/Unix ist für die Durchführung des beschriebenen Recommendation Scans ein Agent erforderlich.

**Für welche Systeme ist Deep Security besonders geeignet?**
Insbesondere für den Einsatz in virtuellen Umgebungen unter VMware vSphere ist das Produkt Deep Security geeignet.
Die agentenlose Umsetzung einer Intrusion Prevention und Detection Lösung bietet hier die meisten Vorteile. Dabei ist es egal, ob es sich um virtualisierte Server oder um eine VDI-Umgebung handelt. Insbesondere bei virtualisierten Desktops bietet sich hierdurch die Möglichkeit mit einem sehr geringen Verwaltungsaufwand auch eine große Anzahl an Systemen zuverlässig zu schützen.

# Dell Expo Tour 2015

Hamburg, 02.06.2015

Dell präsentierte auch in diesem Jahr auf der Dell Expo Tour wieder das komplette Portfolio seiner innovativen End-to-End-IT-Lösungen. IT-Verantwortliche konnten sich über das gesamte Hardware-, Software- und Service-Angebot informieren und erfahren, wie Unternehmen von Zukunftstechnologien wie Software Defined Datacenter, Desktop- Virtualisierung und zuverlässigen Sicherheitslösungen profitieren. BASYS war auch dieses Jahr wieder vor Ort.

Wir fanden: Im Gegensatz zum üblichen Betrieb auf Großmessen hatten wir viel Zeit für individuelle Gespräche. Besucher konnten Produkte live erleben und ausprobieren. Die Veranstaltung haben wir dabei flexibel gestaltet und auf eine feste Agenda verzichtet. Für individuelle Fragen und Diskussionen zu technologischen Trends und Lösungen sind alle DELL Experten vor Ort, das heißt- zahlreiche Möglichkeiten zum Austausch und Networken. Wir freuen uns, auf das nächste Jahr- vielleicht dann ja auch mit Ihnen!

# VMware 6- What`s New am 30.04.2015

Pat Gelsinger, der CEO von VMware, bezeichnete den Release von vSphere 6 und Virtual SAN 6 als eines der wichtigsten Ereignisse der Unternehmensgeschichte von VMware. Die Rund 600 neuen Features wollten wir unseren Kunden mit einer Live Demo präsentieren und luden 2 Systemingenieure von VMware ein. Wir möchten uns für die anregende Diskussion bei unseren Gästen bedanken. Ein großer Dank gilt auch VMware für die tolle Unterstützung.


BASYS EDV – SYSTEME

**Impressum**

**Herausgeber**
BASYS Bartsch EDV-Systeme GmbH

**Kontakt**
Hermine-Seelhoff-Str. 1-2
28357 Bremen
Dr. Stephan Michaelsen
Tel: 0421/43 42 030
stephan.michaelsen@basys-bremen.de

**Geschäftsführer**
Dr. Stephan Michaelsen, Olaf Brandt
HRB 11898



# TechDemo mit NetApp und veeam


Nichts ist spannender als innovative Technologien in der praktischen Anwendung kennen zu lernen. Erleben Sie die Vorteile und Möglichkeiten der neusten Storage-, Backup- und Replikations-Technologien von NetApp und Veeam in einer spannenden TechDemo.
An nur einem Vormittag erhalten Sie einen komprimierten und zugleich umfassenden Überblick zu aktuellen Storage-Trends, Innovationen, Technologien und Einsatzbereichen. Gemeinsam mit unseren Partnern von NetApp und Veeam zeigen wir Ihnen, wie ein „Always on!“ Rechenzentrum auch für den Mittelstand realisierbar und bezahlbar ist.

Wir freuen uns über Ihre Anmeldung. Senden Sie einfach eine E-Mail mit Ihren Kontaktdaten an:

veranstaltungen@basys-bremen.de

NetApp™

VEEAM IT JUST WORKS!™