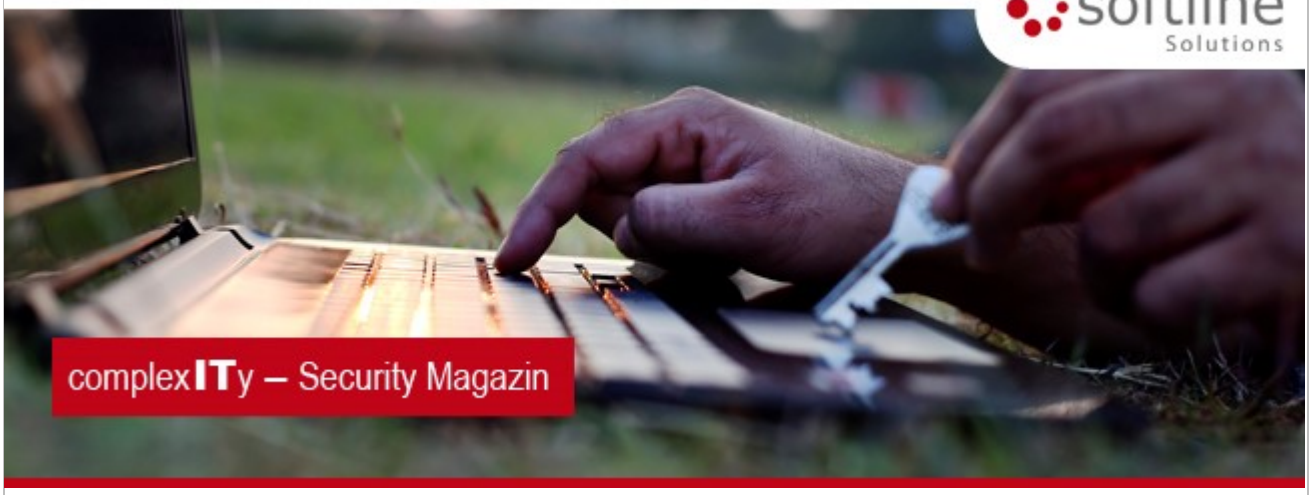

Leipzig, 17.06.2015

Liebe Leserinnen und Leser,

in der zweiten Ausgabe des **IT-Security eMagazins »complexITy«** beschäftigen wir uns mit dem weitverzweigten Themengebiet der **Netzwerkabsicherung**. Seien Sie gespannt auf technische und organisatorische Tipps zur Absicherung Ihrer Systeme und erhalten Sie Einblicke in unsere ganz persönlichen **Best-Practice** Ansätze. **Ankündigungen von Produkten** aus dem Security-Umfeld sind erneut Teil des eMagazins.

Mehrausgaben in IT-Sicherheit und Datenschutz

NIFIS-Studie: In Zeiten immer neuer Bedrohungsszenarien verstärken deutsche Unternehmen ihre Maßnahmen gegenüber Wirtschaftsspionage und Cyberkriminalität. Dieses Bewusstsein hat sich seit dem Beginn der Enthüllungen von Edward Snowden (Anfang 2013) gravierend verändert. Durch das erhöhte Sicherheitsbedürfnis steigen die Ausgaben für IT-Sicherheit und Datenschutz drastisch an. NIFIS hat in einer aktuellen Studie untersucht wie sich deutsche Firmen zu diesen Themen positionieren. Die wichtigsten Ergebnisse finden Sie hier »

Gesetze und Normen

IETF – sicherer TLS-Einsatz: Kürzlich erschien der RFC 7525 von IETF, der Empfehlungen, Vorgaben und Richtlinien für den sicheren Einsatz von TLS definiert. Empfohlen wird:

Ausschließliche Bereitstellung (serverseitig) von TLS 1.2 – sofern keine älteren Clients aus Kompatibilitätsgründen bedient werden müssen.

Einsatz von HSTS zur Erzwingung von HTTPS.

Verzicht auf RC4.

Festlegung der allgemeinen Schlüssellänge auf mindestens 128 Bit.

Implementierung & Betrieb

Firewall im Wandel der Zeit: Vor rund 30 Jahren war an die zukünftige Komplexität heutiger Firewall-Systeme nicht zu denken. In den 80er-Jahren begann die Entwicklung mit **einfachen Paketfiltern,** die nur nach Source/Destination-Address und Service unterschieden. Mitte der 90er Jahre konnte dank der **»Stateful Inspection Firewalls«** besser auf die Anforderungen komplexer

Kommunikationsverbindungen eingegangen werden. Aktuell ist die einstige **»Statefull Inspection Engine«** im Wandel und wird kontinuierlich durch **»Application Filtering«** ersetzt. Perspektivisch ist eine Entwicklung zur **globalen Kommunikation** von unterschiedlichen Sicherheitskomponenten zu erwarten. Mehr Informationen zur Geschichte der Firewall finden Sie auf unserer Webseite »

Netzwerkabsicherung und Klassifikation von Informationen: Zur effizienten Absicherung des firmeninternen Netzwerkes muss bekannt sein, wo sich die relevanten Informationen befinden und wie wertvoll sie für das Unternehmen sind. Hier kann das Augenmerk beispielsweise auf die Zugriffsrechte einzelner Nutzer, die Netzwerkinfrastruktur und die Einhaltung des Datenschutzes gelegt werden. In unserer Checkliste finden Sie die wichtigsten Punkte auf einen Blick.

Benötigen Sie Unterstützung bei der Absicherung Ihres Netzwerkes oder bei der Klassifikation von Informationen? Unsere Experten stehen Ihnen gern mit Rat und Tat zur Seite. Senden Sie einfach eine E-Mail an it-sicherheit@softline-group.com und vereinbaren Sie einen Gesprächstermin!

Best Practice

Firewall-Verwaltung: Die Firewall ist ein wichtiger Pfeiler im Sicherheitskonzept einer jeden Organisation. Umso mehr Sorgfalt sollte man bei ihrer Administration walten lassen. Hier können leicht kleine Fehler unterlaufen, die eine große Wirkung haben und so nicht nur jedem IT-Administrator das Leben schwer machen, sondern darüber hinaus zu erheblichen Sicherheitslücken in Unternehmen führen. Wir stellen Ihnen deshalb auf unserer Webseite die wichtigsten Aspekte bei der Verwaltung Ihrer Firewall vor.

Erfahrungsbericht: Die Aufgabenstellung einer unserer Kunden bestand darin, die alte Microsoft Forefront TMG Hardware Firewall / Proxy, deren Mainstream Support im April ausgelaufen war, durch einen neuen Firewall-Hersteller abzulösen.

Die Ansprüche des Kunden konnten am besten von einem der führenden Anbieter in diesem Sektor, Palo Alto Networks, erfüllt werden. Nach umfangreicher Analyse- und Implementierungsphase wurde das neue System nach insgesamt acht Wochen erfolgreich in Betrieb genommen. Was die Firewall von Palo Alto auszeichnet und wie wir im laufenden Betrieb den Firewall Change Prozess vollziehen konnten, lesen Sie hier »

FAQ – Was bedeutet eigentlich…?

Network Access Control: Um ein Netzwerk und dessen beinhaltende Informationen auch bei Zulassung von heterogenen, oftmals auch autonomen Clients zu schützen, empfiehlt sich der Einsatz von Network Access Control (NAC). Es ermöglicht eine benutzerbasierte Authentisierung von Clients und eine gleichzeitige Durchsetzung von Sicherheitsrichtlinien, wobei Clients, die diese Richtlinien nicht erfüllen, komplett oder teilweise im Netzwerk isoliert und unter Quarantäne gestellt werden können. Als Richtlinie sind hierbei vorrangig technische Vorgaben wie das Datum der Signaturen eines Virenscanners, das Vorhandensein eines bestimmten Sicherheitsupdates oder einer speziellen Software zu verstehen. Durch NAC soll die Wahrscheinlichkeit verringert werden, dass sich ein mit Malware befallener Client mit dem Netzwerk verbinden kann und so unbewusst Schaden im Netzwerk anrichtet.

Network Security Monitoring: Eine effiziente, wenn auch leider nicht vollständig automatisierbare Technologie zur Abwehr bzw. Entdeckung von Angriffen ist das Network Security Monitoring (NSM). Obwohl es viele Parallelen zu klassischen Intrusion Dection bzw. Prevention Systemen (IDS/IPS) besitzt, stellt es keine bloße Erweiterung dar. Während IDS/IPS i. d. R.

Netzwerkverkehr lediglich an einer Stelle im Netzwerk auf Anomalien bzw. bekannte schädliche Signaturen analysieren und automatisiert reagieren kann, besteht ein NSM aus einer Sammlung von mehreren verteilten Sensoren im Netz. Somit gibt es z. B. in jedem Netzwerkabschnitt einen Sensor zzgl. Sensoren vor der Datenbank, Dateisystem etc., die eine aggregierte Auswertung der Aktivitäten im gesamten Netzwerk ermöglichen. Dies umfasst zusätzlich die Analyse der Informationen zur Erkennung von Zusammenhängen, um Indizien sowie Warnung für mögliche Einbrüche schnellstmöglich zu melden. Allerdings ermöglicht NSM keine automatische Reaktion auf mögliche Einbrüche, da es lediglich zur Verbesserung der Sichtbarkeit von Abläufen im Netzwerk dient, weshalb ein menschliches Eingreifen stets von Nöten ist.

Softline Services

Firewall-Penetrationstest: Damit bei Ihnen nix anbrennt, können Sie zum kleinen Preis von **499 € zzgl. MwSt.** einen großen Schritt zu mehr IT-Sicherheit in Ihrem Unternehmen machen: In unserem Firewall Penetrationstest analysieren wir Ihr bestehendes Firewall- oder Gateway-System auf mögliche Schwachstellen. Sie erhalten im Anschluss einen ausführlichen Bericht mit **weitreichenden Handlungsempfehlungen** zur Konfiguration Ihrer Firewall – damit Sie in einem sehr frühen Stadium und ohne große Aufwände das Optimierungspotential Ihrer Installation erkennen und nutzen können. Sind Sie interessiert, die Schwachstellen Ihrer Systeme ausfindig zu machen? Dann senden Sie uns bitte eine E-Mail an it-sicherheit@softline-group.com.

Sonstiges

Breaking News: Die Produkte XenApp und XenDesktop 7.6 von **Citrix** erhalten Common Criteria Zertifikat und besitzen native FIPS 140-2 Compliance.

NEU! VMware vSphere 6.0

„Instant Clone“ zum effizienten Klonen und Bereitstellen virtueller Maschinen

NVIDIA GRID vGPU ermöglicht vom Hypvisor gesteuerte gemeinsame direkte Nutzung des GRID

Höhere Skalierbarkeit, Verbesserung unterstützter Hardware

Übliche Leistungs-, Stabilitäts- und Softwarequalitätsverbesserungen

NEU! VMware Horizon 6.1

In Verbindung mit vSphere 6.0 Nutzung der NVIDIA GRID vGPU-Technologie

Authentisierung bei RDS Desktops mittels Smartcard

Unterstützung für IPv6, Virtual SAN 6.0, Virtual Volumes

Unterstützung für 3rd-Party SSO-Verwaltung von Anmeldedaten

Übliche Leistungs-, Stabilitäts- und Softwarequalitätsverbesserungen

Falls Sie Fragen oder Hinweise zu gewünschten Magazininhalten haben oder unsere Unterstützung in IT-Sicherheitsprojekten benötigen, dann kontaktieren Sie uns unter it-sicherheit@softline-group.com oder telefonisch unter +49 341 24051-0.

Mit freundlichen Grüßen

Ihr Softline Team.

Softline Solutions GmbH // Geschäftsführer: Martin Schaletzky // Sitz der Gesellschaft: Leipzig // Handelsregister Leipzig: HRB 26058 // Steuer Nr.: 232/118/06001 // USt ID: DE270894910