Ausgabe 03.2015

Inside ACP

Der Newsletter der ACP IT Solutions

Weitere Themen dieser Ausgabe:

- **Sophos Unified Threat Management**
- **Ciscos neue Generation von Sicherheitslösungen**
- **SonicWALL: Sicherheitslösungen für alle Größen**

TOPTHEMA: CYBER-SECURITY

IT-SICHERHEIT:
Ist der Kampf bereits verloren?

Die Cyberattacke auf den Bundestag hat gezeigt: Selbst hochgesicherte Einrichtungen verlieren gelegentlich den Kampf. Experten befürchten, dass große Teile der Hardware getauscht werden müssen.

Ein wesentlicher Bestandteil heutiger Schutzmechanismen basiert auf der Abwehr bekannter Gefahren, bzw. der Erkennung von Mustern. Dabei gehören Zero-Day-Attacken (der Virus verbreitet sich schneller als das Update des Scanners) längst zum Alltag. Die eigentliche Gefahr kommt jedoch aus einer anderen Ecke. Profi-Hacker setzen nicht auf eine massenhafte Verbreitung von Viren, Würmern, Trojanern und ähnlichen Schädlingen, sondern entwickeln zielgerichtete, objektfokussierte Angriffswaffen.

Das bedeutet, die verwendeten Schadcodes werden nur selten eingesetzt und daher von musterbasierten Erkennungssystemen nicht erfasst. Solange sie nicht entdeckt werden, bleiben sie unsichtbar. Einmal im Netz, verbreiten sie sich innerhalb kooperierender Kontaktgruppen – unabhängig von Firmengrenzen und Standorten.

Im Gegensatz zu den meisten Einbrüchen der realen Welt hinterlassen Hacker nur selten Spuren. Wer sicher sein möchte, setzt auf Systeme zur Erkennung von Anomalien. Am gebräuchlichsten sind dabei Netzwerk-basierte Intrusion-Detection-Systeme (IDS und IPS). Diese scannen den Datenverkehr nach auffälligen Paketen und ungewöhnlichen Verbindungen.

In den meisten Fällen geht jedoch den Einbrüchen das Fehlverhalten eines oder mehrerer Mitarbeiter voraus. Um dieses Risiko zu minimieren, beginnen immer mehr Unternehmen mit entsprechenden Sensibilisierungsmaßnahmen. Schulungen sind sinnvoll, auf lange Sicht aber keine Lösung. Wenn es ausreicht, Webseiten aufzurufen und Dokumente zu öffnen, um ein Netz zu infiltrieren, wird auf Dauer jede Barriere fallen.

Langfristig helfen nur elementare Veränderungen. Seit Jahrzehnten orientiert sich die Internetbranche am technisch Machbaren. Die Frage sollte sein: Welche Geräte, Anwendungen und Dokumente benötigen wir tatsächlich für unser rechnergestütztes Arbeiten? Gefahren-Hotspots wie z.B. Personalabteilungen tragen ein besonders hohes Risiko, da hier viele Dokumente unbekannter Herkunft eingehen. Nicht immer ist ein uneingeschränkter Datenverkehr wirklich erforderlich bzw. sinnvoll. Manchmal wäre es besser, verschiedene Unternehmensbereiche stärker voneinander abzuschotten.

Das ACP-Expertenteam hat hierzu einen Security-Check entwickelt, mit dem der Sicherheitsstand im Unternehmen geprüft, Schwachstellen aufgedeckt und dann geeignete Maßnahmen ergriffen werden können.

Mehr dazu finden Sie unter www.acp.de/securitycheck

Trend Micro-Studie

Banking-Malware DYRE wieder auf dem Vormarsch

Nutzer von Online-Banking in Deutschland, Österreich und der Schweiz fühlen sich in der Regel sicher. Starke Authentifizierungsmechanismen und kaum Schadsoftware sind der Grund für dieses Gefühl. Online-Gangster wollen das ändern und weiten ihre Angriffe auf Anwender auch in Zentraleuropa deutlich aus – mit runderneuerten Schädlingen, die sich gut zu tarnen wissen und nicht nur Online-Banking-Daten abgreifen.

Auszeichnung

ACP gewinnt EMEA Award von NetApp

ACP hat beim diesjährigen NetAPP EMEA Partner Executive Forum in Warschau eine der Hauptkategorien – Clustered Data ONTAP – gewonnen. ACP hat im kürzlich abgeschlossenen Geschäftsjahr 2015 erneut Rekorde in der Kooperation mit NetApp erreicht und eine sehr große und breite Basis an installierten Systemen – sowohl in Österreich wie auch in Deutschland – erzielt. Das hervorragende Ergebnis wurde nun prämiert.

Amando Software

ACP SAM-Team setzt auf Miss Marple

Ein wesentlicher Bestandteil eines SAM-Audits ist die Erfassung der installierten Lizenz-Basis. Miss Marple Lizenzkontrolle von Amando Software bietet eine einfache und effiziente Möglichkeit, alle tatsächlich genutzten Programme unternehmensweit zu ermitteln und Lizenzen zu verwalten oder sogar zu sperren. Die Möglichkeiten der Lizenzverwaltung reichen dabei vom Lizenzmetering und der Kontrolle von Serverinstallationen, Terminalclients, lokal installierter Software bis hin zur Verwaltung von Software-Suiten wie Microsoft Office.

Cyberspionagekampagne „Grabit“ attackiert mittelständische Unternehmen

Kaspersky Lab enthüllt Details zur Cyberspionagekampagne „Grabit“, die es in erster Linie auf kleine und mittelständische Unternehmen und Organisationen aus den Bereichen Chemie, Nanotechnologie, Bildung, Landwirtschaft, Medien und Bauwesen abgesehen hat. Auch Firmen in Deutschland und Österreich sind betroffen.

Die Grabit-Angreifer versenden E-Mails mit einem angeblichen Microsoft-Word-Anhang. Sobald ein Mitarbeiter den Anhang herunterlädt, wird über einen gehackten Remote-Server ein Spionageprogramm auf seinem System installiert. Es kommen ein Keylogger von HawkEye sowie ein Konfigurationsmodul inklusive zahlreicher Fernwartungs-Tools (Remote Administration Tools) zum Einsatz.

Beachtliche Ausbeute

Ein von Kaspersky Lab analysiertes Keylogger-Programm von nur einem Command-and-Control-Server (C&C-Server) war in der Lage, 2.887 Passwörter, 1.053 E-Mails und 3.023 Nutzernamen von 4.928 verschiedenen infizierten Systemen zu stehlen – neben Bankkonten wurden auch Daten von Outlook, Facebook, Skype, Google Mail, Pinterest, Yahoo, LinkedIn und Twitter entwendet.

Bei Grabit sind einerseits keine großen Anstrengungen zu erkennen, die eigenen Aktivtäten zu verbergen. So untergraben etliche eingesetzte Schädlinge die eigene Sicherheit, indem sie denselben Hosting-Server und zum Teil sogar dieselben Zugangsdaten nutzen. Andererseits setzen die Hintermänner auch starke Verschleierungstechniken ein, um ihren Code vor Sicherheitsexperten zu verbergen. Kaspersky Lab geht daher davon aus, dass hinter der Spionageoperation eine lose Gruppierung steht, bei der einige Teile eher technisch versiert und somit schwerer aufzuspüren sind als andere. Zudem deuten Analysen darauf hin, dass nicht alle Codes vom selben Malware-Programmierer geschrieben wurden. Die Lösungen von Kaspersky Lab erkennen und schützen vor allen Grabit-Varianten.

Sophos Unified Threat Management

Im Markt befinden sich heute eine ganze Reihe von Anbietern, die damit begonnen haben, eine Vielzahl von Security-Funktionen in einer Appliance zu bündeln. Doch trennt sich die Spreu vom Weizen. Sophos bietet ein solides, leistungsstarkes Gesamtpaket, das trotz seiner umfangreichen Schutzfunktionen vergleichsweise einfach und intuitiv zu bedienen ist.

Der Schutz des Netzwerks basiert auf mehrschichtigen, bewährten Schutztechnologien wie Advanced Threat Protection (ATP), IPS, VPN, E-Mail- und Web-Filterung. Jede Funktion ist auf allen Appliance-Modellen aktivierbar.

Administration und Konfiguration erfolgen über den kostenlosen Sophos UTM Manager. Hier werden auf einfachste Weise für ein oder mehrere Appliances Richtlinien erstellt und überwacht. Die integrierte Reporting-Engine gibt zudem einen detaillierten Überblick über entsprechende Echtzeit- und Vergangenheitsdaten.

Das Herz der Appliance ist jedoch die Next-Gen Firewall. Sie legt fest, welche Anwendungen gesperrt, erlaubt und priorisiert werden sollen. Die Identifizierung der Applikationen erfolgt via Deep-Packet-Inspection (Layer 7).

Mit Sophos RED (Remote Ethernet Device) können außerdem externe Standorte sicher angebunden werden. Sophos RED ist das erste Security Gateway, für das kein technisches Fachwissen am Remotestandort erforderlich ist. Einmal installiert, leitet Sophos RED den Datenverkehr an die UTM weiter und schafft umfassende Sicherheit. Sophos UTM fungiert außerdem als Wireless-Controller, d.h. Access Points werden automatisch eingerichtet und erhalten umfassenden UTM-Schutz.

Sophos UTM 625:
Komplettschutz für große Unternehmensnetzwerke

Cisco stellt neue Generation von Sicherheitslösungen vor

Laut Cisco waren alle für den Cisco 2015 Annual Security Report untersuchten Unternehmen mit Malware infiziert. So dynamisch die aktuelle Bedrohungslandschaft ist, so weist sie doch eine Konstante auf: Angreifer entwickeln und verbessern ständig neue Technologien, um ihre schädlichen Aktivitäten vor den Sicherheitslösungen zu verbergen. Mit zwei neuen Sicherheitslösungen will Cisco dieser Entwicklung gegensteuern.

AMP Everywhere
Mit Advanced Malware Protection erhalten Kunden leistungsfähige Werkzeuge für eine schnellere Entdeckung und Behebung von Vorfällen. Neue Funktionen für Threat Intelligence, dynamische Malware-Analyse und rückwirkende Sicherheit für Cisco AMP erhöhen den Schutz vor, während und nach einem Angriff. AMP Threat Grid bietet dynamische Malware-Analyse und Threat Intelligence durch seine fortschrittliche Analytics Engine, die Security-Teams bei der Untersuchung und Einschätzung von Sicherheitsvorfällen unterstützt. Die erweiterten Funktionen stehen als Cloud Services sowie auf Cisco UCS Appliances auch on-premise zur Verfügung.

FirePOWER Services
Cisco ASA mit FirePOWER Services bietet eine hohe Flexibilität mit standardisiertem, einheitlichem Management der einzelnen Installationen. Sie kombiniert die Überwachung von Zugangsrichtlinien mit Funktionen für Advanced Threat Protection. Die FirePOWER Services von Cisco bieten eine mehrstufige Sicherheitslösung, die eine umfassende Transparenz mit vielen neuartigen Nachweisverfahren kombiniert. Die Lösung markiert auch bislang unbekannte Malware und verkürzt damit die Zeit bis zu deren Entdeckung und Behebung von Wochen auf Stunden.

Als Cisco Goldpartner unterstützen ACP und SWS ihre Kunden bei Auswahl, Einführung und Betrieb von Cisco Security - Lösungen.

> Hinter dem Oberbegriff Malware verbergen sich: Viren, Trojaner und Würmer, Flooding und DoS- und DDoS-Attacken, Spyware, Spams, Hoaxes, Rootkits usw.

UNIFIED THREAT MANAGEMENT

SonicWALL: Sicherheitslösungen für Unternehmen aller Größen

Mit der Übernahme von SonicWALL im Jahr 2012 schloss DELL seine Lücke im Bereich Sicherheitslösungen. Die von SonicWALL entwickelten Produkte eignen sich für Unternehmen und Organisationen jeder Größenordnung.

Die Next-Generation-Firewalls von SonicWALL sind ein essentieller Bestandteil intelligenter und anpassungsfähiger Sicherheitssysteme. Dabei lassen sie sich so skalieren, dass auch wachsende und verteilte Unternehmensnetzwerke extrem sicher sind. Die Security Appliances von SonicWALL können auch als Unified Threat Management (UTM)-Firewalls genutzt werden.

Ausgerichtet auf die Mobilitätsanforderungen einer modernen Unternehmenskultur, verfügt SonicWALL zudem über eine ganze Reihe an Secure Mobile Access-Lösungen. Damit erhalten Geschäftsreisende, ausgestattet mit Notebooks, Tablet-PCs und Smartphones, einen nahezu uneingeschränkten, sicheren Zugriff zu geschäftskritischen Ressourcen.

Mit der SonicWALL Continuous Data Protection (CDP)-Serie können Unternehmen Daten problemlos aufbewahren, replizieren, archivieren, kontrollieren und wiederherstellen. Neue, ausgeklügelte Funktionen optimieren die Datensicherung und Datenverwaltung.

SuperMassive E10800:
Network Security Appliance für Rechenzentren

Die Verwaltungs- und Reporting-Lösungen von SonicWALL bieten eine umfassende Architektur für die zentrale Erstellung und Verwaltung von Sicherheitsrichtlinien, eine echtzeitbasierte Überwachung, Analysen des Datenverkehrs sowie das Erzeugen intuitiver Berichte. Die Lösungen sind für kleine und mittlere Unternehmen genauso geeignet wie für Konzerne mit verteilten Standorten oder Managed Service Provider.

Interview mit Florian Oelmaier

Leiter IT-Sicherheit & Computerkriminalität, IT-Krisenmanagement bei Corporate Trust

Herr Oelmaier, die Corporate Trust ist Dienstleister im Bereich Unternehmenssicherheit. Zu Ihrem Spezialgebiet gehört auch das Thema Cybersicherheit. Wie stufen Sie die aktuelle Sicherheitslage ein und was empfehlen Sie den Unternehmen?
Die IT-Sicherheitslage hat sich radikal verändert. Dieser Wandel hat nicht im Bereich der IT-Sicherheitslücken stattgefunden – diese sind im Wesentlichen gleich geblieben: alte wurden geschlossen, neue gefunden. Die IT-Sicherheitsanstrengungen wurden intensiviert, dafür sind Vernetzung und Komplexität gestiegen. Der signifikante Wandel hat im Bereich der Täter und deren Motivation stattgefunden. Noch vor 10 Jahren waren die Täter Skriptkiddies und IT-Nerds, motiviert durch Geltungsbedürfnis und Selbstverwirklichung. Heute dominieren organisierte Kriminalität, Geheimdienste, Cyber-Söldner und wohl bald auch Terroristen das Geschehen. Unsere Empfehlung: Machen Sie sich bereit, auch signifikante Änderungen in Ihren Verteidigungsstrategien in Betracht zu ziehen.

Sie stellen fest, dass nicht mehr alle Bereiche eines Unternehmens gleichermaßen abgesichert werden können. Was meinen Sie damit?
Die meisten Unternehmen denken in drei Sicherheitszonen: Internet, DMZ und Intranet. Das reicht nicht mehr aus. Ein durchschnittliches Unternehmen braucht heute 6 bis 8 Zonen mit unterschiedlichem Sicherheitsniveau. Die Frage, welche Daten welchen Schutzbedarf haben, muss dabei das Business beantworten. In einer solchen Struktur werden dann auch komplexere Sicherheitslösungen wie SIEM, IDP und ein 100%-Log für die höchste Schutzzone handhab- und bezahlbar.

Wo sehen Sie die Schnittstelle zur ACP?
Die Corporate Trust – Business Risk & Crisis Management GmbH versteht sich als Berater und Partner in Krisen- und Notfallsituationen. Eine solche Krisensituation ist ein laufender Cyberangriff bzw. die Entdeckung eines bereits abgeschlossenen Informationsabflusses. In solchen Fällen ergänzen wir mit unserem Know-how rund um Angriffsaufklärung, Täterverfolgung, IT-Forensik und Krisenmanagement die ACP-Experten beim Kunden vor Ort.

UNSERE PARTNER (Auszug):

Cisco · Citrix · DataCore Software · DELL · DeskCenter Management Suite · EMC² where information lives · IBM · Fortinet · Fujitsu · hp · Kaspersky Lab · KEMP Technologies · lenovo · Microsoft · NetApp · Samsung · Sophos · Trend Micro · Veeam · vmware

TERMINE

30. Juli 2015
München: Workshop ACP Safebox

23. September 2015
Hauzenberg: Microsoft-Lizenzierung

24. September 2015
Regensburg: Microsoft-Lizenzierung

21. Oktober 2015
Hauzenberg: 3. Security Forum

22. Oktober 2015
Regensburg: 3. Security Forum

IHR REGIONALER ACP-KONTAKT IN DEUTSCHLAND

Bad Tölz
Tel.: 08041-799988-0
E-Mail: bad-toelz@acp.de

Frankfurt
Tel.: 06109-69691-0
E-Mail: frankfurt@acp.de

Hannover
Tel.: 0511-35777-0
E-Mail: hannover@acp.de

Hauzenberg (SWS Computersysteme AG)
Tel.: 08586-9604-0
E-Mail: info@swsnet.de

Kolbermoor
Tel.: 08061-9089-0
E-Mail: kolbermoor@acp.de

Köln
Tel.: 0221-66992-0
E-Mail: koeln@acp.de

Markdorf
Tel.: 07544-50399-0
E-Mail: markdorf@acp.de

München
Tel.: 089-358980-0
E-Mail: muenchen@acp.de

Regensburg (SWS Computersysteme AG)
Tel.: 0941-20605-0
E-Mail: info@swsnet.de

Stuttgart
Tel.: 0711-23917-0
E-Mail: stuttgart@acp.de

Sulzbach/Taunus
Tel.: 06196-56142-0
E-Mail: sulzbach@acp.de

Ulm
Tel.: 0731-141151-0
E-Mail: info.ulm@acp.de

HERAUSGEBER:
ACP Holding Deutschland GmbH
Stuttgarter Straße 3-5
80807 München
E-Mail: inside_acp@acp.de