Kommunikationstechnik für Profis

funkschau

Ausgabe 1-2/2014 31. Januar 2014 € 6,00 sfr 10,00

funkschau.de

Telekommunikation Datensicherheit

Sonderdruck: EWE swb osnatel Vertrauen verbindet.

ITK-INVEST

Einkaufsführer zu Trends und ITK-Produkten

ab Seite 51

„Und schon sind wir auf seiner Platte!“

Eigentlich sieht er ganz nett aus. Aber man sollte sich von den gewienerten Schuhen und dem zuvorkommenden Verhalten nicht täuschen lassen, Mark Semmler ist gefährlich. Ein Hacker. Ein Mann, der zum Spaß Viren programmiert, der Sätze sagt wie: „Willst du die 4.000 meistbenutzten Passwörter? Kann ich dir geben!“ – Keine Frage, der 40-Jährige könnte im Netz Furchtbares anrichten, wenn er auf der dunklen Seite der Macht stehen würde. Tut er aber nicht! Stattdessen setzt der Geschäftsführer der Darmstädter IT-Sicherheitsfirma Antago seine Fähigkeiten für etwas Gutes ein – die Informationssicherheit von Unternehmen. Regelmäßig sind IT-Fachleute und Geschäftsführer verschiedener Unternehmen seine Zuhörer. Sie folgen der Einladung von Firmen zum Thema „Managed-Security“.

Wie wirkungsvoll die „echten Bösen“ im Netz arbeiten, zeigt Semmler gleich zu Beginn eines solchen Abends: „Willkommen beim Livehakking“: Schwungvoll tippt er auf seiner Tastatur herum, murmelt Sachen wie „Punkt, Slash, 16“, drückt Enter und schon rattert auf seinem Rechner eine Liste an ungeschützten Servern herunter. Raunen im Publikum. „Das sind Firmen, die ohne funktionierende Firewall im Netz herumturnen!“ Getuschel. „Hier: SBS-DC-001, das ist der Domaincontroller, den guten Mann haben wir damit bei den Königsnüssen.“ Sprachlosigkeit. „Oder Büro-Server, ungeschützt im Netz!“ Fassungslosigkeit. Die sich nochmals steigert, als Semmler berichtet, wie er einmal den offenen Ordner einer Arztpraxis entdeckt habe, in dem alle eingehenden Faxe automatisch als PDFs abgelegt waren. „Ich konnte 2.500 Krankenakten einsehen!“

Weiter geht's: „smbclient, gib mir mal Infos zu diesem Kandidaten“, sagt Semmler und attackiert so einen fremden Rechner. Passwort? Nicht nötig, einmal Enter reicht, um diese „Hürde“ zu nehmen. „Und siehe da, schon sind wir auf seiner Platte!“ Das Publikum ruft gleichermaßen erschrocken wie fasziniert die Ordnernamen durch den Raum, auf die ein Zugriff möglich wäre: „My eBooks“, „Zahllasten“, „Überweisungen“, „Urlaubsbilder“.

Da Semmler ja nur den Bösen spielt, öffnet er keinen dieser Ordner. Wohl aber legt er einen neuen namens „Aaaaaaargh“ an, um demnächst dem Chef der Sanierungs-Firma, die die Webseite betreibt, die eklatanten Sicherheitslücken zu verdeutlichen. Und darauf hinzuweisen, dass er auch Neonazi-Propaganda hätte abspeichern können. „Kleines Quiz: Wird das Material entdeckt, wer bekommt dann wohl arge Probleme?“, fragt Semmler in die Runde. Richtig, der Sanierer.

Schutz durch Firewall

Nun gibt es gegen Hacker-Angriffe keinen 100-prozentigen Schutz, Technik-Lücken können immer auftreten. Dem Gefängnis oder der Geldstrafe kann ein Unternehmer trotzdem entgehen, das Zauberwort ist „Verkehrssicherungspflicht“: Wer eine Gefahrenquelle unterhält, muss zumutbare Vorkehrungen treffen, um Schäden anderer zu verhindern. „Das gilt fürs Schneeschippen auf dem Gehsteig vor Ihrer Haustür wie für Ihre IT-Infrastruktur“, so der Security-Experte. Ob Mitarbeiter über den Arbeitsrechner illegal Musik und Filme herunterladen oder sich Hacker Zutritt zum Server verschaffen, Firmengeheimnisse stehlen und damit Dritten schaden. Stets muss der Geschäftsführer nachweisen, dass er Vorkehrungen getroffen hat, um das zu verhindern – sonst haftet er persönlich. Aber wie funktioniert das?

„Hiermit“, übernimmt Markus Bittner. Er steht neben Semmler und deutet auf einen kleinen Kasten. Bittner ist Mitglied des „Competence Centers Security & LAN“ von Ewe Tel und nimmt an der Veranstaltung teil, um Beispiele für gemanagte Sicherheitslösungen zu zeigen. Der Kasten beinhaltet eine dezentrale Firewall von Ewe Tel samt dem Unified-Threat-Management-Paket (UTM) mit Antiviren, Antispam, Web- oder Contentfilter. Diese Technik kann zum einen Hacker-Angriffe abwehren, zum anderen interne Zugriffe auf vorab festgelegte Seiten im Web unterbinden.

Für größere Unternehmen, die einen zentralen Internet-Ausstieg besitzen, bietet Ewe Tel alternativ eine zentrale Firewall als gehostete Lösung im hochverfügbaren konzerneigenen Rechenzentrum in Oldenburg an. „Unter Beibehaltung derselben Sicherheitsstandards und Funktionalitäten wie bei der dezentralen Firewall arbeiten wir hier auf Basis eines virtuellen Systems, das uns die Nutzung von Synergie-Effekten erlaubt, und deshalb kosteneffektiver ist“,

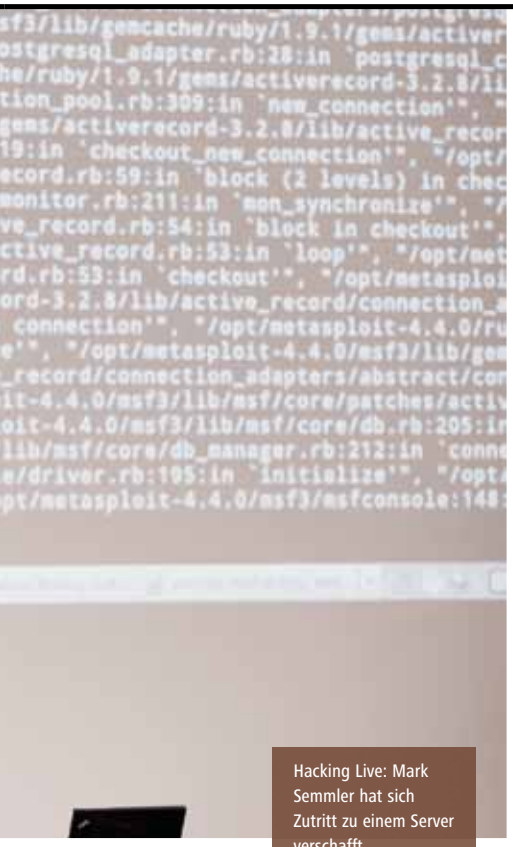

Bild: Ewe Tel

Hacking Live: Mark Semmler hat sich Zutritt zu einem Server verschafft.

erläutert Bittner einige der Vorteile. Weiterer Benefit für die Kunden: Die zentrale Firewall wird immer als hochverfügbares Cluster ausgelegt, so dass zwei identische Systeme sich kontinuierlich untereinander abgleichen und den Administrator bei Unregelmäßigkeiten alarmieren.

Updates, Updates, Updates

„Na, dann wollen wir mal gucken, wie gut deine Kiste ist", sagt Semmler zu Bittner und haut wieder in die Tasten. Von der Hackerwebseite oxid.it holt er sich die App „Cain und Abel" – „und die ist böse mit großem B!" Sie entschlüsselt Passwörter, zieht aus dem Datenverkehr die Credentials, speichert VoIP-Telefonate als Audiodateien ab, die sich der Hacker anhören kann. Nach diesen Erläuterungen lässt Semmler „Cain und Abel" auf Bittners Rechner los – doch dessen Firewall blockt den Angriff lässig ab.

Ob Firewall oder Anti-Virus-Programm. Zu diesem Thema hat Semmler fünf wichtige Wörter zu sagen: „Updates, Updates, Updates, Updates, Updates!" Ein Aspekt, an den Unternehmen nicht denken müssen, die mit Bittner und seinen Kollegen zusammenarbeiten. „Die gesamte Soft- und Hardwarepflege inklusive aller Updates der Sicherheitssysteme übernehmen wir", informiert er – während seine Firewall nebenbei den „rechnung.februar.exe"-Angriff abwehrt, den sein Nebenmann unterdessen gestartet hat.

Gleiches gelingt Minuten später wieder, als Semmler den Exploit auf den Ewe Tel-Rechner schleudert, mit dem vor einigen Monaten die Sicherheitslücke des Internet Explorers ausgenutzt werden konnte. „Gute Firewall, klasse konfiguriert", lobt Semmler anschließend Bittners kleine Box. Apropos: „Ob eine Firewall gut ist, liegt nicht nur am Aufkleber auf der Packung, sondern auch am Können desjenigen, der sie konfiguriert", sagt Semmler. Und das reiche seiner Meinung nach oftmals nicht aus. „Besucht der Mitarbeiter einer kleinen IT-Klitsche einen dreitägigen Workshop, ist er noch lange kein Sicherheitsexperte! Die Zeit der Amateure ist vorbei, dafür sind die Hacker zu ausgebufft."

Tipps zu Managed-Security

Wichtiger erster Schritt: Identifikation der Kronjuwelen
Welches sind die entscheidenden Werte und Informationen des Unternehmens und wo befinden sie sich? Tipp: Fragen Sie sich, welche Mindestanforderung zum Erfolg des Unternehmens zwingend erfüllt werden muss. Konzentrieren Sie sich zunächst auf das Wesentliche und verfeinern Sie dann.

Risiko-Analyse: Wo und in welcher Form können Probleme auftauchen?
Welche IT-Systeme verwalten welche Informationen? Welche Bedrohungen/Schwachstellen sind denkbar? Welcher Schaden könnte entstehen? Tipp: Versuchen Sie, potenzielle Schäden möglichst konkret zu beziffern, um sie dem Einsatz für Sicherheitsressourcen gegenüber stellen zu können.

Manpower-Planung: Wieviel „Mitarbeiter" braucht mein Sicherheits-Konzept?
Welche personellen Ressourcen benötigen Sie, damit Sicherheitsthemen erkannt, eingeschätzt und bearbeitet werden können? Tipp: Überlegen Sie, welche Aufgaben zwingend intern besetzt werden müssen und welche outgesourct werden können. Fragen Sie sich: Kann und will ich es selbst tun?

Prozesse festlegen: Alle Stationen berücksichtigen
Welche Prozesse sind erforderlich, damit das Thema Sicherheit angemessen gemanagt werden kann? Tipp: Legen Sie diese Prozesse fest und überlegen Sie, welche Parteien eingebunden und welche Kontrollen eingebaut werden müssen. Erstellen Sie auch Notsysteme und entsprechende Notfallpläne.
Bedenken Sie sowohl technische als auch organisatorische Maßnahmen. Stellen Sie Regeln auf und überprüfen Sie deren Einhaltung.

Kontinuierliche Verbesserung: Aus Fehlern lernen
Wie können Sie gewährleisten, dass erkannte Sicherheitsvorfälle nicht erneut zum Problem werden? Tipp: Verbessern Sie die bereits etablierten Sicherheitsprozesse und -maßnahmen fortlaufend und scheuen Sie auch nicht davor zurück, sie umzustrukturieren oder neue hinzuzunehmen, wenn Sie dadurch schneller und effektiver reagieren können. Werten Sie Ihre Alarmprotokolle aus, um Problembereiche zu identifizieren. Leiten Sie Maßnahmen ab, wo nötig und sinnvoll.

Vorsicht bei der Auswahl von Anbietern: Achtung, Dumping-Angebote!
Haben Sie Security-Komplettangebote erhalten und fragen sich, wo der Unterschied zu teuren Anbietern liegt? Tipp: Klären Sie unbedingt ab, welches Landesrecht gilt und dass Ihre sensiblen Daten darunter nicht dem Sammler gehören!

Zentral: Professionelle Sicherung Ihrer Hard- und Software
Entsprechen Ihre Sicherungssysteme den aktuellen Standards? Tipp: Schützen Sie Ihre Daten und die dazugehörige Hardware, beispielsweise durch ausgereifte Zutrittskontrollen in Rechenzentren. Sichern Sie Ihre Daten elektronisch gegen Angriffe aus dem Internet. Prüfen Sie, ob ein System, das sensible Daten bearbeitet, wirklich aus dem Internet erreichbar sein muss. Sorgen Sie aber auch für die Aufklärung aller Mitarbeiter, wie man einen Sicherheitsvorfall erkennt und wie und wo man ihn meldet.

Was ist Trumpf in Sachen Sicherheit? Compliance-Regularien beachten
Haben Sie auch alle geltenden Gesetze und Spielregeln beachtet und erfüllen Sie Ihre Verkehrssicherungspflicht? Tipp: Verpflichten Sie auch hierfür intern oder extern Fachleute.

Alexander Schmolke,
freier Redakteur

Katja Schmitt-Völsch,
Ewe Tel

Der Safe für Ihre Daten

Regionale Sicherheitslösungen für Unternehmen

Wir bieten Ihnen maßgeschneiderten Datenschutz für Ihr Unternehmen – kompletter Service natürlich inklusive.

Firewall-Lösungen – Datensicherheit für Ihr Unternehmen

Nahezu jedes Unternehmen in Deutschland ist schon einmal Ziel von Cyberattacken gewesen. Große Unternehmen melden sogar mehrere Angriffe pro Woche. Das zeigt, wie wichtig es ist, dass Unternehmen sich schützen. Wir helfen Ihnen, Ihre Daten wirkungsvoll vor Trojanern, Viren, Botnetzen, Phishing und Spam zu schützen:

- **Professionelle und maßgeschneiderte Firewalls**
- **Konfiguration, Monitoring und Management durch hochqualifiziertes Personal**
- **Automatische Sicherheits-Updates**
- **Optional: UTM - Unified Threat Management (Antivirus, Antispam und weitere Sicherheitsdienste)**

Rechenzentren in Ihrer Region – höhere Verfügbarkeit für Ihre IT

In unseren hochverfügbaren Rechenzentren in Oldenburg und Osnabrück sind Ihre Daten sicher aufgehoben. Hier bieten wir Ihnen breitbandige, dedizierte Anbindungen an unseren Glasfaser-Backbone. Nutzen Sie modernste Technologien, ohne sie selbst betreiben zu müssen. Konzentrieren Sie sich auf Ihr Kerngeschäft!

- **Professionelles Sicherheitskonzept – Standorte z. T. mit TÜV-IT-Zertifizierung (bis zu Level 3 erweitert)**
- **Höchste Sicherheit vor Stromausfall, Feuer, Einbruch und Hochwasser**
- **Skalierbar von Höheneinheiten bis zu mehreren 19''-Schränken**
- **Kalkulierbare IT-Kosten und Kostentransparenz**
- **Hohe Diensteverfügbarkeit durch breitbandige Internetanbindung**
- **Remote Hands durch qualifiziertes Personal**
- **Auf Wunsch gesicherter Out-of-Band-Zugang**

Infos unter 0800 589 5464 (kostenfrei)

EWE TEL GmbH
Cloppenburger Straße 310
26133 Oldenburg

EWE swb osnatel Vertrauen verbindet.