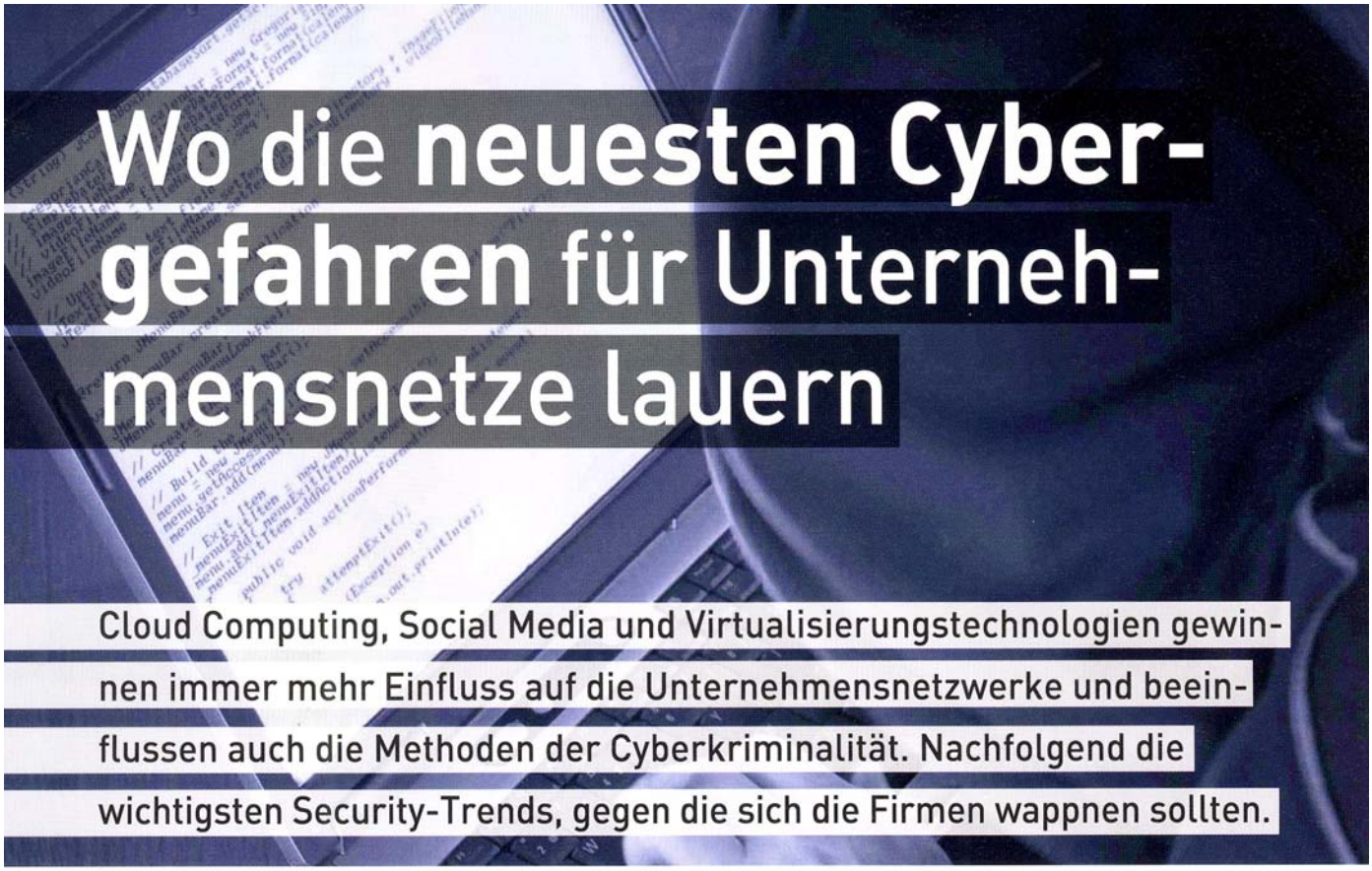
Publication: ICT kommunikation (CH)
Publishing House: Kapi-Media Verlag
Publication date: 25.02.2010
Page: 24-25



Wo die neuesten Cyber-gefahren für Unterneh-mensnetze lauern

Cloud Computing, Social Media und Virtualisierungstechnologien gewinnen immer mehr Einfluss auf die Unternehmensnetzwerke und beeinflussen auch die Methoden der Cyberkriminalität. Nachfolgend die wichtigsten Security-Trends, gegen die sich die Firmen wappnen sollten.

IT-Security steht bei den IT-Verantwortlichen nach wie vor weit oben auf der Agenda. Der Grund: Malware und Cyberattacken lassen die CSOs (Chief Security Officer) nicht zur Ruhe kommen. Nachfolgend die zentralen Trends im Sicherheitsbereich, über die die Unternehmensanwender Bescheid wissen sollten, um entsprechende Gegenstrategien in die Wege leiten zu können.

Security in virtualisierten Umgebungen

Der Schutz virtueller Umgebungen erfordert nicht nur die Absicherung der physischen Perimeter, sondern auch der Interaktion zwischen virtuellen Geräten. Wird eine neue virtuelle Maschine erstellt, können sich Infektionen über Kreuz ausbreiten. Unternehmen müssen daher sicherstellen, dass die Security-Richtlinie für den Perimeter nicht für die virtuelle Umgebung gilt, sondern der virtuellen Bewegung der Server folgen.

Informationszentrierte Security

Im nächsten Jahrzehnt wird es verstärkt auf eine informationszentrierte statt eine netzwerkzentrierte Security ankommen, da Daten zunehmend ausserhalb traditioneller Unternehmensnetzwerke verfügbar sein werden. Die Definition von «Netzwerk» umfasst nicht mehr nur das LAN, sondern auch verteilte Netzwerke, Cloud-basierte Netzwerke, Social-Media-Netzwerke, Mobilfunknetze, virtuelle Netzwerke usw. Daten müssen über die Netzwerkinfrastruktur hinaus geschützt werden, indem an jedem Datenberührungspunkt oder internen Netzwerkabschnitt Security-Kontrollen eingerichtet sind und nicht nur am Perimeter. Informationszentrierte Security stellt im Gegensatz zur netzwerkzentrierten Security einen granularen, intelligenten und vielschichtigen Ansatz dar, der den schwächsten Punkt im Netzwerk gegen Angriffe schützt.

Security in Cloud-Umgebungen

Cloud-Services konfrontieren Unternehmen mit zahlreichen Risiken und Schwachstellen. Daten werden über öffentliche Kanäle zwischen einzelnen Netzwerken hin- und hergeschickt, was die Möglichkeiten für Infektionen oder Betrug steigert. 2010 wird der Schutz der Cloud mehr denn je ein Thema sein, da immer mehr Unternehmen Services wie Miet-Storage, Software as a Service, virtuelle IT und Application Hosting einführen. Die Frage, wie ruhende Daten und Daten in Bewegung geschützt werden können, zwingt Unternehmen dazu, verschiedene Security-Mechanismen zum Schutz ihrer Daten zu

Infos zum Autor

Franz Kaiser
Country Manager Austria, Switzerland and Central Eastern Europe, Fortinet

prüfen, wie zum Beispiel Verschlüsselung, SSL-Inspection, Data Leakage Prevention und Antivirus.

Mehrschichtige Application Control

Die immer beliebter werdenden Social-Media-Applikationen bringen neue Gefahren mit sich. Das stellt vor allem für Unternehmen eine Gefahr dar, deren Mitarbeiter solche Applikationen auch privat über das Firmennetzwerk nutzen. Erst kürzlich richteten «Koobface» und «Secret Crush» Schaden auf Millionen Seiten von Facebook und Myspace-Nutzern an. 2010 wird sich der Bereich Application Security deutlich weiterentwickeln und intelligente, mehrschichtige Security-Kontrollen hervorbringen. Damit können granulare Richtlinien für einzelne Applikationen definiert werden, um bestimmte Applikationsschichten zuzulassen oder zu blocken. Zudem können zugelassene Applikationen nach gefährlichen Aktivitäten überprüft und diese direkt am Gateway abgefangen und beseitigt werden.

Netzwerkfunktionalitäten für Security-Geräte

Die Konsolidierung von Netzwerk-Services wird auch 2010 bei budgetbewussten Kunden auf Akzeptanz stossen. WAN-Acceleration hat sich als integriertes Feature in konsolidierten Security-Lösungen bereits etabliert. Gutartiger Datenverkehr kann so beschleunigt und bösartiger effektiv geblockt werden. Switching und VoIP sind Netzwerk-Services, die als nächstes in konsolidierte Security-Lösungen integriert werden könnten.

Crime-as-a-Service (CaaS) vs. Security-as-a-Service (SaaS)

Cyberkriminelle lassen sich immer mehr vom neuen Security-as-a-Service-Modell inspirieren und führen ihr eigenes Crime-as-a-Service-Modell ein, um Hacker oder ganze Umgebungen für kriminelle Handlungen zu vermieten. Security-as-a-Service wird beliebter, da Unternehmen die komplexe Aufgabe der Netzwerkabsicherung an Service-Provider übertragen können. Die Vorteile liegen auf der Hand: Kosteneffektivität und Einfachheit. Aufgrund dessen wird SaaS auch weiter im Trend liegen – ebenso wie Crime-as-a-Service. Cyberkriminelle erweitern damit ihre Reichweite und können zudem ihre Identität vertuschen.

Im laufenden Jahr ist mit einem deutlichen Zuwachs an so genannten «Crime Kits» zu rechnen, also Bausätzen, die über die zentralisierte Systemsteuerung eines Botnetzbetreibers bösartige Netzwerke anonym steuern und verwalten können. Diese «Crime Kits» werden sich 2010 noch weiterentwickeln und schliesslich Wartungsleistungen, Hilfestellungen und Q&A-Support durch kriminelle Interessengemeinschaften integrieren. Die derzeit gängigste CaaS-Methode ist die Anmietung von Netzwerken für die Verteilung von Malware, Adware oder Spam. Service-Angebote wie Beratungsleistungen und die Vermietung von Hackern für DDoS-Angriffe, das Stehlen von Informationen und Erpressung von politischen Parteien, Regierungen, Unternehmen und Bürgern sind im Kommen.

Scareware und Ransomware

Verbraucher wissen sich immer besser vor Scareware zu schützen. Eigentlich ein gutes Zeichen. Da die hohe Lukrativität gefälschter Security-Software lockt, werden Cyberkriminelle dennoch neue Mittel und Wege finden. Ransomware beispielsweise verschlüsselt Daten und Dateien und macht sie dadurch unbrauchbar. Erst gegen Lösegeldzahlungen, oftmals per MMS, erhalten die Opfer den Schlüssel zur Wiederherstellung der Daten.

Neue Methoden der Geldwäsche

Auch neue Geldwäschemethoden liegen in der Luft. Im Vordergrund stehen dabei die Rekrutierung und Nutzung von Geldwäschern – meist ahnungslosen Einzelpersonen – anhand innovativer, professioneller Stellenausschreibungen. Cyberkriminelle werden sich darauf konzentrieren, die Identität der Geldwäscher zu verschleiern. Mithilfe von Authentifizierungstechniken erhalten Ermittler und Behörden, die mit kriminellen Netzwerken in Kontakt treten, gezielt falsche Informationen. Echte Informationen etwa zu Geldwäschekonten laufen nur über authentifizierte Verbindungen.

Microsoft und andere Plattformen im Visier der Verbrecher

Mit der steigenden Nutzung neuer Plattformen werden Cyberkriminelle ihre Angriffe über Microsoft Windows hinaus ausbreiten. Insbesondere zwei Faktoren sorgen für Angriffe auf andere Plattformen. Zum einen bieten plattformübergreifende Applikationen wie zum Beispiel Flash, Javascript usw. ein erhöhtes Angriffsrisiko und zahlreiche Ziele. Zum anderen haben es Hacker auf die Ausbeutung dieser Plattformen abgesehen. Schwachstellen in mobilen Plattformen und Komponenten wie MMS-Nachrichten auf dem iPhone oder bösartiger Code in Symbian-OS wurden bereits entdeckt. Für 2010 ist hier mit weiteren Möglichkeiten und Methoden zu rechnen.

Botnetz-Angriffe

Bei Botnetz-Angriffen wird es nicht mehr nur um die Verschleierung ihrer binären Codes gehen, sondern verstärkt um legitime Kommunikationsmittel wie seriöse Protokolle, Datenverschlüsselung und Authentifizierungstechniken. Botnetz-Aktivitäten über Twitter und Google-Gruppen wurden bereits entdeckt – Tendenz steigend. □