IT-SOFTWARE

NAC-Echtzeitlösung

Die Business Security Assurance Solution Suite (BSA) des israelischen Entwicklers Sysob ist in der Version 5.0 erschienen. Mit dem System ist die Absicherung des Netzwerks mittels einer Kombination von aktiven und passiven Erkennungsmethoden möglich. Als wesentliche Neuerung der Echtzeitlösung zur Netzwerkerkennung und -zugangskontrolle (NAC) wird die komplette Neuerstellung des Management Centers genannt, welches nun auch Updates auf mehrere Kollektoren über ein einzelnes Interface verteilen kann.

Neues von Turfin

Neue Massstäbe beim Security Lifecycle Management sollen sich mit den beiden Turfin-Technologies-Lösungen Securetrack 4.5 und der Security Suite setzen lassen. Die Security Suite besteht aus Securetrack 4.5 und Turfin Securechange Workflow und soll Unternehmen leistungsstarke Funktionen zur aktiven Steuerung und Kontrolle im Security Lifecycle Management bieten – und das weitgehend automatisiert. Securetrack 4.5 seinerseits kann mit Funktionen wie On Demand Compliance Reporting aufwarten oder Compliance White Listing, um über Policies zu regeln, welche Art von Datenverkehr zulässig ist. Ausserdem sei die Lizenzierung vereinfacht worden.

Sage erneuert Act

Act, die Kunden- und Kontaktmanagement-Software aus der Schmiede von Sage, ist in der Version 2009 auf den Markt gekommen. Nebst einer gesteigerten Performance, welche sich insbesondere durch schnelleres Synchronisieren von Dateianhängen bemerkbar macht, verspricht der Hersteller zahlreiche weitere Verbesserungen. So können doppelt angelegte Gruppen- und Firmenkontakte nun gesucht und in der Listenansicht entfernt werden, und die Datenbank kann von Doubletten gesäubert werden. Daneben wurde an der Suchfunktion der CRM-Lösung geschraubt, so dass sich Informationen schneller finden lassen.

Verschlüsselung für Kleine

Die PGP Corporation hat mit PGP Whole Disk Encryption Workgroup Edition eine nach eigenen Angaben einfach zu bedienende und preisgünstige Lösung für den Verschlüsselungsschutz von Datenträgern vorgestellt, die speziell für den Schutz sensibler digitaler Informationen in kleinen und mittleren Unternehmen konzipiert und entwickelt wurde.

Sicherheit in konvergenten Netzen

Die ersten Netz-Konvergenzkonzepte gehen bis in die 30er Jahre zurück. Erst das Internet hat die Konzepte Realität werden lassen. Damit wurden auch neue Sicherheitskonzepte nötig: Ein Rück- und Ausblick.

Von Fabien Dombard

In der Geschichte der Telekommunikation tauchen die ersten Konvergenz-Konzepte in den 30er Jahren bei AT & T auf. Doch erst gegen Ende des zwanzigsten Jahrhunderts machte die Digitalisierung der Kommunikation die Umsetzung dieser Konzepte wirklich möglich: Zuerst für Unternehmen, dann auch für Privatpersonen. Während den letzten 20 Jahren hat das Internet als globalisiertes Netzwerk den Austausch von Text-, Audio- und Video-Material revolutioniert. Erst das Internet als eigenständiges Medium hat die Versprechen der Konvergenz einlösen können.

Doch der Segen ist auch Fluch: Der ungebändigte Informationsaustausch führte zu einem bisher nicht gekannten Ausmass von Sicherheitsproblemen. Auch hier reagierten zuerst Unternehmen auf das Problem, mittlerweile nutzen aber auch Privatpersonen Sicherheitsvorkehrungen wie Antivirenprogramme oder Firewalls. Auch der Schutz persönlicher Daten – beispielsweise bei Bankzahlungen – ist mittlerweilen im Privatsektor angekommen.

Konvergenz birgt neue Risiken

Konvergenz in der Telekommunikation – und da sind wir beim Thema Unified Communications – bringt neue Sicherheitsrisiken. Brauchten wir früher vor allem die Kontrolle über E-Mails, brauchen wir jetzt die Kontrolle über das ganze Netz. Dabei können wir die Erfahrung, die wir beim Sichern von Textkommunikation gesammelt haben, auf den Schutz von Sprachkommunikation anwenden. Zumindest teilweise: Denn Medienkonvergenz über IP (oft vereinfacht als Telecommunication over IP oder Toip bezeichnet) ist um einiges schwieriger zu handhaben als textueller Kommunikationsaustausch. Das betrifft sowohl Bedienerfreundlichkeit als auch Sicherheit.

Die Problematik lässt sich am besten mit einem Blick in die Vergangenheit verbildlichen: Es ist noch nicht allzu lange her, als jedes Medium sein eigenes Netzwerk benutzte, um Informationen zu transportieren. Die Netze galten als sicher, weil sie von Natur aus geschlossen waren. Die Systeme waren zudem proprietär, die entsprechenden Dokumentationen wurden vor den Augen der Konkurrenz so gut als möglich versteckt. Aus der Sicht des Telekommunikations-Anbieters bestand Sicherheit darin, Externen den Zugang zum intern operierenden Netzwerk zu verweigern. Die Endbenutzer hatten lediglich Zugriff zu einem Endgerät mit sehr eingeschränkter Funktionalität. Zudem gehörte das Endgerät oftmals dem Provider. Die Kupferleitung, die nur Sprache und ein sehr eingeschränktes Befehleset zwischen dem Endbenutzer und dem lokalen Switch ermöglichte, war ein gegebener Medienbruch. Dementsprechend änderte sich die Sicherheitsproblematik nur selten und in langsamen Zyklen.

Die Nomaden sind die treibende Kraft

Wahrer Auslöser der Konvergenz war schliesslich erst die Mobilität. Das Verlangen und nach Nomadismus bei den Endbenutzern war die treibende Kraft, die schliesslich zum Umbau der Telekommunikationsstrukturen geführt hat. Das Internetprotokoll IP hat sich dabei aus zwei Gründen als einziges Transportmittel durchgesetzt: Einerseits wegen seiner technischen Möglichkeiten, andererseits aber sicher auch wegen seiner Kostengünstigkeit.

Die daraus resultierende Verbindung der Netze hat auch die Sicherheitsproblematik radikal geändert. Da auf diesen verbundenen Netzen mit bekannten, oft offenen und dokumentierten Protokollen gearbeitet wird und dabei auch bekannte und weit verbreitete Betriebssysteme zum Einsatz kommen. Daraus entstanden neue Netzwerk-Topologien, die auch unter dem Namen New Generation Networks (NGN) bekannt sind. Diese neuen Strukturen stellen auch neue Anforderungen an alle Beteiligten: An die Netzwerkbetreiber, an Hardware-Verkäufer und an die Endnutzer.

Einmal angreifen genügt

Ein grosses Problem ist einerseits das Ressourcen-Management. Weder Sprache noch Video erträgt eine Latenzzeit. Doch die grössten Probleme betreffen Sicherheitsaspekte. Durch die Zusammenführung von neuen Geräten und Applikationen auf eine Plattform entsteht ein zentraler Schwachpunkt mit unzähligen Attackiermöglichkeiten. Gleichsam gefährdet sind die Vertraulichkeit der Netze und die Privatsphäre der Benutzer. Kommt hinzu, dass die Erkennungsmethoden für unberechtigte Zugriffe in NGN-Architekturen, die verschiedene Netze von verschiedenen Betreibern verschmelzen lassen, komplizierter sind. Auch neue Arten von Denial-of-Service-Attacken werden auftreten, oder Spam kann künftig auch einfacher über Internet-Telefonie verbreitet werden.

Viele Probleme kriegt man heute schon in den Griff. Geräte, die auf Sub-Protokoll-Ebene agieren, werden implementiert. Richtig geführt kann Technologie-Konvergenz auch in der Sicherheit einiges an Vereinfachung bringen. Mehr als je zuvor muss dabei allerdings das Sicherheitskonzept bereits auf dem Produkt- und Infrastruktur-Level einfliessen. Die verschiedenen Komponenten müssen dieselbe Sprache sprechen. Und zukünftige Netzwerke werden über SEM (Security Event Management) und SRM (Security Resources Management) verfügen müssen. Dazu gehören einerseits Sicherheitsaudits, eine Netzwerkpolitik für Compliance und eine Netzwerk-Supervision. Andererseits rücken technische Lösungen wie Konfigurations-Management, Ressourcen-Management sowie Zugangs- und Zonen-Kontrolle in den Mittelpunkt.

DER AUTOR

Fabien Dombard (28) ist französischer Branch Manager beim Schweizer Sicherheitsunternehmen Oneconsult. Er arbeitet seit über neun Jahren in der IT-Branche und verfügt über Projekt- und Beratungs-Erfahrung im Sicherheitsbereich. Seine Spezialität sind Applikations-Audits, Penetrations-Tests, Reverse Engineering sowie Voip-Sicherheit.