Sichere Kommunikation mit der Zentrale

Bankfilialen sind ganz besonders auf sichere Verbindungen mit der Zentrale angewiesen.

Die Informationstechnik spielt im Markt für Finanzdienstleistungen eine tragende Rolle und hat sich zu einem wichtigen Wettbewerbsfaktor entwickelt. Die simultane Bereitstellung von Informationen an jeden Ort weltweit unterstützt neue Vertriebskanäle und sorgt dafür, dass alle Mitarbeiter vom Wissensstamm des Unternehmens profitieren können. Was Banken online nach außen präsentieren, ist nur ein Bruchteil von dem, was intern an Informationen und Diensten zur Verfügung steht. Mitarbeiter nutzen Portale zur Urlaubsplanung, spezielle B2B- und B2C-Portale stehen für ausgewählte Kundenkreise offen. Natürlich darf es keine Rolle spielen, ob die Mitarbeiter, die die Dienste nutzen und pflegen, in der Zentrale oder einer Außenstelle beheimatet sind. Allerdings sind die Sicherheitsanforderungen bei der Anbindung von Bankfilialen an die Zentrale enorm hoch. Das fängt schon bei der Verfügbarkeit an, weil die gemeinsame Datenbasis zentral vorgehalten wird und Filialen ohne Netzwerkverbindung von den Kundendaten abgeschnitten wären. Natürlich spielt auch die Sicherheit gegen Angriffe von außen eine große Rolle. Wurde früher die Online-Anbindung über dedizierte Standleitungen aufgebaut, die eine Punkt-zu-Punkt Verbindung ermöglichten, wird heute, vor allem bei kleineren Außenstellen, auch das Internet in Kombination mit starker Verschlüsselungstechnik genutzt. Damit muss ein Sicherheits-Gateway auch die Abwehr der üblichen, mittlerweile automatisierten, Techniken wie Port- oder Vulnerability-Scanning beherrschen. Filialen haben meist noch das zusätzliche Handicap, dass sie über kein ausgewiesenes Personal verfügen, dass sich um die IT-Infrastruktur kümmert. Ein Gateway muss also zum Einen wartungsarm, zum Anderen auch aus der Ferne einfach zu konfigurieren und kontrollieren sein.

Die Appliance als Lösung

Appliances bieten sich an, wenn Komplettlösungen gesucht werden, die schnell installiert und ohne großen Folgeaufwand laufen sollen. Weil sie über kein separates Betriebssystem verfügen, fällt dessen Konfiguration weg. Auch das so genannte „Härten" von Treibern und Diensten ist einfacher, weil die Funktion der Appliance genau festgelegt ist. Nicht benötigte Komponenten werden gelöscht oder abgeschaltet, die Basis der Appliance bleibt so klein und fehlerresistent wie möglich. Einige Anbieter gehen sogar so weit, den sonst zum Management eingesetzten HTTP-Dienst abzuschalten. Für das Management liefern diese Hersteller eine eigens programmierte Anwendung mit; mögliche Sicherheitslücken in den diversen Web-Servern müssen den Anwender nicht kümmern. Unerlässlich ist, dass die Managementapplikation mehrere Appliances verwalten kann, selbstverständlich über verschlüsselte Verbindungen. Unter Umständen sind einige Hundert Filialen mit dem Sicherheits-Gateway ausgestattet, es sollten also größere Mengen von Geräten zu Gruppen zusammengefasst werden können. Die Konfiguration wird sehr erleichtert, wenn der Sicherheits-Admin Schablonen mit Default-Einstellungen an alle Geräte einer Gruppe verteilen kann. So beschränken sich Änderungen auf die Arbeit an einem Gerät, der Rest der Gruppenmitglieder bekommt alle Einstellungen über die Schablone zugewiesen. Das die Managementanwendung auch unterschiedliche Modelle der Security-Appliance verwalten kann, gehört zum guten Ton bei seriösen Anbietern. Schließlich ist es in großen Netzwerken sehr wahrscheinlich, dass nicht nur ein Modell einer Security-Appliance eingesetzt wird, sondern, je nach Filialgröße unterschiedlich große und performante Systeme. Das führt zu einem weiteren KO-Kriterium: Skalierbarkeit. In den letzten Jahren gab es für die Systemanforderungen und das Datenaufkommen nur eine Richtung – nach oben. Banken beobachten eine enorme Ausweitung des Transaktions- und Datenvolumens, das bewältigt werden muss. Dabei kann zum Einen Skalierbarkeit innerhalb einer Plattform helfen. Das Übertragungsmedium legt in vielen Fällen die Gesamtleistung des Sicherheits-Gateways fest. Kann man nachträglich von einer ISDN- oder Frame-Relay Leitung auf einen Anschluss per xDSL aufrüsten, steigt der Durchsatz um mehrere Größenordnungen. Dabei muss immer die Redundanz berücksichtigt werden. Praktisch jede Zweigstelle wird über mindestens zwei Leitungen angebunden, wenn irgend möglich auch über zwei getrennte Provider. Ist das nicht durchführbar, muss zumindest eine Backup-Verbindung im Notfall dazuschaltbar sein, auch wenn sie langsamer ist als das Standardmedium. Selbst kleine Security-Appliances sollten diese Anforderungen erfüllen; sobald mehr als eine Handvoll Mitarbeiter in der Außenstelle arbeiten, steigen die Leistungsanforderungen nochmals deutlich an. Hier ist es wichtig, dass der Hersteller auch Gateways für Zentralen oder Niederlassungen mit Konzentratorfunktion im Angebot hat. Nur so bleibt die Verwaltung des Gesamtsystems simpel und überschaubar. Knappen Durchsatz

kann man aber auch durch Planung und Kontrolle vermeiden. Umfangreiche Quality-of-Servive Funktionen sorgen in einer guten Security-Appliance dafür, dass die verschickten Pakete mit der passenden Priorität bearbeitet werden. Wird bereits Voice-over-IP eingesetzt, haben Sprachdaten Vorrang vor HTTP-Informationen. Geschäftskritische Anwendungen, die beim persönlichen Kundenkontakt genutzt werden, müssen schneller zu ihren Daten kommen, als eine Textverarbeitung.

Historie nicht vergessen

Der Trend geht zwar zu offenen Standards, doch in vielen Banken sind nach wie vor Legacy-Anwendungen im Einsatz und werden das auch auf absehbare Zeit bleiben. Eine Security-Appliance muss auch mit nicht-TCP/IP Protokollen zu Rande kommen, wenn diese zu wichtigen Legacy-Anwendungen gehören. Natürlich wird darüber hinaus erwartet, dass alle gebräuchlichen Kommunikationsprotokolle wie SMTP und POP3 verarbeitet werden können. Auch wenn ein Mailserver in der Regel in der Zentrale betrieben wird, rufen die Mitarbeiter ihre E-Mails über die Security-Appliance ab, ein direkter Internetzugang ist in Filialen praktisch nie vorgesehen oder gewünscht. Darum muss das Gateway mit den Paketen korrekt umgehen können. Anti-Spam- und Anti-Virus-Funktionalität gilt dagegen eher als „nice-to-have" Feature. Die Mails werden bereits in der Zentrale gecheckt, Spam verworfen. Falls doch aus einem Grund in der Filiale Viren und unerwünschte Mails gesiebt werden sollen, sind Application-Proxys hilfreich. Sie bilden für die Außenwelt den einzigen Kontaktpunkt und stellen sicher, dass jede Mail auf Datenpaketebene untersucht und falls nötig verworfen wird.

Sicherheit hört natürlich nicht bei Spam und Viren auf. Die Firewall in der Appliance muss klar regeln, wer und welche Anwendung Zugriff auf die internen Ressourcen hat. Und gerade wenn kein Administrator vor Ort ist, um bei Warnmeldungen sofort im Netzwerk nach dem Rechten zu sehen, leistet ein Intrusion Prevention System (IPS) wertvolle Dienste, indem verdächtige Verbindungen blockiert und beendet werden. Dass trotzdem eine Echtzeit-Benachrichtigung an den Admin herausgeht, ist selbstverständlich. Doch eine Benachrichtigung bei Gefahr ist längst nicht alles, was ein modernes Sicherheits-Gateway im Bankenumfeld beherrschen muss. Analyse- und Statistikfunktionen mit grafischer Aufbereitung gehören ebenso dazu wie der klassische Syslog-Daemon, der Meldungen an ein Protokolliersystem schickt. Informationen über Datenaufkommen und Auslastung der Verbindungsmedien sollten online in Echtzeit zur Verfügung stehen, aber auch als Datei exportiert werden können, um Erweiterungen bei der Filialanbindung gegenüber dem Management zu vertreten.

Eine der wichtigsten Aufgaben des Security-Gateways ist der Schutz der Verbindung zur Gegenstelle. Das gilt sowohl für die Anbindung an die Zentrale, als auch für einzelne Accounts, wenn sich Mitarbeiter von außerhalb in das Netzwerk einloggen. Ein solider VPN-Server ist die Grundlage, auf der alle weiteren Schutzmaßnahmen aufbauen. Deutsche Hersteller wie die Securepoint GmbH, die keinen Exportbeschränkungen bei Kryptographie unterworfen sind, können RSA-Verschlüsselung mit bis zu 1024 Bit langen Keys anbieten. Üblich sind sonst 256 Bit Länge. Zudem sorgt ein automatisches Key Management (AKM) für schnellen und sicheren Schlüsseltausch. Generell gelten IPsec VPN-Verbindungen als komplex und schwierig einzurichten. Ganz wird sich die Komplexität nie auflösen lassen, doch Wizards, die die Eingaben auf Plausibilität prüfen und nur sinnvolle Werte zulassen verhindern Leichtsinnsfehler und lange Fehlersuche.

Sichtbare Sicherheit

Was viele Nutzer großer, verteilter Sicherheitsarchitekturen beklagen, ist die Unübersichtlichkeit der überlappenden und zusammen hängenden Regeln und Maßnahmen. Eine grafische Darstellung der Security-Policies, in der Verknüpfungen klar werden und Abhängigkeiten leicht zu sehen sind, hilft. Sie sorgt auch bei über lange Zeit gewachsenen Strukturen für korrekte Zugriffsrechte und ein schlankes Regelwerk. Noch besser ist es, wenn der Administrator beim Regel-Update durch Plausibilitätskontrollen und Optimierungsläufe unterstützt wird. Die Policies können dabei nicht nur Geräten sondern auch Benutzern zugeordnet werden. Die Berechtigungen folgen dem Mitarbeiter also innerhalb des Netzwerks, wenn er an einem anderen Arbeitsplatz sitzt oder sich gerade in der Zentrale aufhält.

Sicherheit und Vertrieb

In der Finanzdienstleistungsbranche geht im Moment ein Strukturwandel vor sich. Der Wettbewerb wird immer stärker, und zwingt die Unternehmen zu hoher Flexibilität im Produktbereich und Vertrieb. Wirtschaftlichkeitsfragen stehen mittlerweile bei unternehmerischen Entscheidungen weit oben, im Zug der Globalisierung und der Erschließung neuer Zielgruppen müssen die Voraussetzungen für die schnelle Bedienung neuer Vertriebskanäle geschaffen werden. Mit diesen Herausforderungen kann nur ein Unternehmen erfolgreich umgehen, dass über eine leistungsfähige IT-Infrastruktur verfügt. Moderne, standardisierte Kommuni kationstechnologien sind ebenso wichtig wie leistungsfähige Security-Infrastrukturen. Die Bereitstellung von B2C und B2B Plattformen zwingt Banken und deren IT-Dienstleister zu einer umfassenden Integration der Kunden-Infrastrukturen über sichere und standardisierte Schnittstellen. IT-Sicherheit ist daher zu einem kritischen Erfolgsfaktor im Finanz dienstleistungsumfeld geworden. ■

Lutz Hausmann

Geschäftsführer
Securepoint GmbH