

## Sicherheit ist Massarbeit

**Auf der Hitliste der häufigsten Attacken gegen die Finanzindustrie (laut Symantec Internet Security Threat Report) stehen Computer-Wurm-Angriffe zuoberst. Welche Gegenmassnahmen empfehlen Sie Ihren Kunden?**

Zusätzlich zum klassischen «Vulnerability Management» mit Software Patch Updates, Viren-Scanner und Firewalls bietet vor allem eine solide, ganzheitliche IT-Sicherheitsinfrastruktur effektiven Schutz. Eine solche Infrastruktur stützt sich auf ein sicheres Betriebssystem,

**PHILIPP FÄRBER\***

benutzt durchgängig verschlüsselte und authentische Kommunikationskanäle und teilt das Firmennetz in Sicherheitszonen oder so genannte Kompartimente mit klar definierten Policies und Übergängen auf. Generell gilt, dass Attacken umso leichter werden, je einheitlicher Umgebungen konfiguriert sind. An vorderster Front sollte ein authentisierender Entry Server als Reverse Proxy (z.B. nevisProxy) nur kontrollierte Verbindungen aus dem Internet zulassen und damit die Angriffe «klassischer» Würmer abblocken. Würmer, die beispielsweise über neue Sicherheitslücken oder als E-Mail-Attachments trotzdem zur Ausführung gelangen, werden durch adäquate Mechanismen innerhalb der Sicherheitsinfrastruktur (starke Authentisierung, Zonen, Intrusion Detection, Auditing) am Erwerb sensibler Daten und Informationen und an der weiteren Ausbreitung gehindert.

**Die Erfahrung zeigt, dass viele Schädlinge über Home-PC oder Mobilcomputer der Mitarbeiter an der Firewall vorbei ins Firmennetz gelangen. Was ist hier die beste Abwehrstrategie?**

Erstens gilt es, die Benutzer «auszubilden»: Durch klare Informationen und strikte Vorgaben kann das Sicherheitsbewusstsein geschult und ein verantwortungsvoller Zugriff auf das Firmennetz erreicht werden. Der Zugriff sollte dabei nur über firmeneigene, zentral aufgesetzte und kontrollierte Hardware und Software erfolgen.

Zweitens sollte Server-seitig der Online-Zugriff auf Firmendaten nach Möglichkeit ganz vermieden oder nur sehr restriktiv zugelassen werden. Starke Authentisierung (z.B. Smartcards) und die Verwendung von VPN-Technologie sind für Letzteres Pflicht. Meist genügt jedoch der Zugriff auf eine vorgelagerte

Zone ausserhalb des eigentlichen Firmennetzes vollauf (z.B. für WebMail oder Windows Terminalserver).

Drittens muss der «physische» Zugang zum Firmennetz selbst gesichert sein, um potenziell infizierte Systeme fern zu halten. Wünschenswert ist hier eine starke Authentisierung auf Netzwerkebene, doch sind – speziell hinsichtlich der besonders gefährdeten «Wireless Network Access Points» – die jeweiligen Standards noch zu wenig etabliert.

**Spam ist vom blossen Ärgernis zu einem ernst zu nehmenden Sicherheitsrisiko geworden. Mit Spam werden nicht nur Trojaner verschickt und Phishing-Versuche unternommen, hohe Spam-Volumina können auch das System so stark belasten, dass ein geregelter Betrieb verunmöglicht wird. Was lässt sich dagegen tun?**

Eine technisch wirksame Begrenzung der Spam-Flut würde den Umbau eines Grossteils der Mail-Gateways bedeuten – und ist dadurch leider nicht praktikabel. Aktuelle Spam-Filter leisten aber inzwischen gute Arbeit, und durch die Kombination mehrerer Produkte lässt sich die Belastung von internen Systemen und Endbenutzern durch Massen-Mails stark reduzieren.

Demgegenüber stellen die angesprochenen gezielten Angriffe durch Phishing-Mails eine aktuelle Sicherheitsbedrohung dar, die gerade im Kontext von «Online-Banking» relevant ist. In Kombination mit «Pharming», also «man-in-the-middle»-Angriffen über gefälschte Web Sites, bieten hier aber auch relativ sichere Login-Verfahren wie Streichlisten oder Challenge/Response keinen absoluten Schutz.

Neben notwendiger Aufklärungs- und Schulungsarbeit kann ein Dienstleister proaktiv zusätzliche Schutzvorkehrungen treffen: Eine E-Mail an Kunden sollte immer authentisch (also digital signiert) verschickt und das Online-Banking-Portal immer mit SSL geschützt werden – wenn möglich sogar mit Zertifikats-basierter Authentisierung der Benutzer.

**Zu lasche Sicherheitsmassnahmen gefährden das Business und setzen die Vermögenswerte einem hohen Risiko aus; zu rigorose Massnahmen behindern den Betrieb und können ihn im Extremfall zum Stillstand bringen. Wie findet man das richtige Mass?**

Eine funktionierende Sicherheitsinfrastruktur ist unsichtbar. Leider fällt sie gerade deswegen leicht Budgetkürzun-

gen zum Opfer. Verlangt ein Sicherheitskonzept dazu noch «umständliche» Prozesse oder führt ein abgelaufenes Zertifikat sogar zu Betriebsunterbrüchen, so wird Sicherheit allgemein als Einengung empfunden und nach Möglichkeit umgangen.

Deswegen muss beim Aufbau einer Sicherheitsinfrastruktur von Anfang an auf gut integrierte, unkomplizierte und möglichst automatisierte Abläufe geachtet werden. Beim Aufbau einer kundenspezifischen PKI legen wir zum Beispiel grossen Wert auf die betriebliche Integration der Prozesse und bieten mit unserem Zertifikatsmanagement-System nevisCA eine zentrale Bewirtschaftungskomponente. Dies senkt die Kosten und erhöht gleichzeitig die Betriebs-sicherheit und den Benutzerkomfort. Parallel dazu müssen die Sicherheitsvorkehrungen für die Benutzer Sinn machen, was sich nur über stetige Aufklärungsarbeit erreichen lässt.

**Seit Jahren besteht der Wunsch, unterschriebene Papierverträge zu ersetzen durch elektronische, die mit digitalen Signaturen versehen sind. Machbar ist das, doch ist es auch praxisgerecht? Und ist es sicher genug für die Finanzindustrie?**

Die Sicherheit digitaler Signaturen ist technisch weitestgehend gewährleistet. Auch in rechtlicher Hinsicht hat die Schweiz dieses Jahr mit dem Signaturgesetz die erforderlichen Grundlagen geschaffen. Die konkreten Anwendungen und Dienste, die signierte Dokumente benutzen, fehlen allerdings noch. Demzufolge mangelt es auch an Erfahrungen im Umgang mit digitalen Signaturen. Dabei wäre ein diesbezügliches Know-how angesichts der offenen Fragen (wie etwa zum Thema der Langzeitarchivierung) eminent wichtig. Gefragt sind Dienstleister, welche die Anwendung digitaler Signaturen gezielt fördern, indem sie zum Beispiel finanzielle Anreize für die Nutzung entsprechender Applikationen schaffen.

Da in der Schweiz die ersten Ausgabestellen erst per Ende Jahr ihre «qualifizierten Zertifikate» anbieten werden, ist es noch zu früh, eine Aussage über deren allgemeine Akzeptanz zu machen. Sobald allerdings eine «kritische Masse» von Dienstleistern, juristischen Entscheidern und Signaturbenutzern erreicht ist, ist mit einer schnellen Verbreitung dieser Technologie zu rechnen.

\* Philipp Färber, Dr. sc. techn. ETH, ist Senior Security Engineer bei der Zürcher AdNovum Informatik.