

Herausforderung Informatik-Sicherheit

Gefahren lauern überall – doch das Management ist sich den effektiven Auswirkungen zuwenig bewusst. Niemand kann es sich mehr leisten, umfassende Informatik-Sicherheitsvorkehrungen zu unterlassen. Umfassende und kostengünstige Sicherheit-Boxes schaffen Abhilfe.

Aldo Britschgi

Die Netz- und Informationssicherheit entwickelt sich immer mehr zu einem Schlüsselfaktor unserer Informationsgesellschaft. Informationen jeglicher Art, bereitgestellt durch weltweite Vernetzungen, nehmen im geschäftlichen und privaten Leben eine immer wichtigere Rolle ein. Denken wir bloss an die Freizeitplanung: Ohne Internet-Anschluss für das Studieren des Online-Fahrplans, Kinoprogramms, Durchführung der Hotel-Reservation oder Erledigung der Bankaufträge über Internet geht nichts mehr – zu selbstverständlich ist ein funktionierender und vermeintlich sicherer Internet-Anschluss. Netze und Informationssysteme transportieren mehr und mehr empfindliche Daten und wirtschaftlich wichtige Informationen, was Anreize für Angriffe drastisch erhöht. Das genaue Ausmass der tatsächlichen und potenziellen Schäden durch Einbrüche in die Netz-sicherheit ist schwer festzulegen. Es existiert kein zentrales Berichterstattungssystem und viele Unternehmen geben natürlich Zwischenfälle aus Angst vor Imageverlusten nicht bekannt.

Steigende Anforderungen

Eines scheint aber sicher: Bereits einschlägig bekannt gewordene Sicherheitszwischenfälle aufgrund von Viren und Hackerangriffen sind vergleichsweise trivial, studiert man die tendenzielle Verlagerung der Angriffe via Benutzerattacken und die bevorstehenden Generationen von multifunktionalen Viren sowie Trojaner der neuen Generation. Sie fragen sich, was dies heissen könnte? Statt ein Dokument zu löschen oder offensichtlich zu verun-

stalten schleicht sich ein Virus in die Excel-Datei und verändert einfach willkürlich ein paar Zahlen. Man merkt vielleicht erst in einem halben Jahr oder noch später, dass etwas nicht stimmen kann. Und mit jeder Korrektur erscheinen die Zahlen noch unwahrscheinlicher. Ihr aktuelles Antivirenprogramm erkennt diesen Virus noch nicht – dieser ist ja noch nicht bekannt. Sind Sie sicher, dass dieser hypothetisch beschriebene Virentrojaner noch nicht auf Ihrem Computer wütet? Gemäss der «IT-Security Studie» stellen

Vorsicht Phishing-E-Mails

Phishing-E-Mails sind betrügerische E-Mails, die den Empfänger zur Preisgabe von persönlichen Angaben auf gefälschten Internetseiten verleiten. Die E-Mails täuschen einen seriösen Absender vor und sind täuschend echt im Layout des vertrauten Absenders gestaltet, verwenden also beispielsweise Logo und Schriftzug der Hausbank. Seien Sie misstrauisch, wenn jemand nach persönlichen Daten fragt, insbesondere nach Bankdaten. «Die Bank verlangt beim Kunden ausnahmslos nie persönliche Angaben per E-Mail oder Telefon» weiss ein Bankenvertreter zu bekräftigen. Also Vorsicht, denn in einem solchem Fall muss es sich zwangsläufig um einen Betrugsversuch handeln.

Viren, Würmer und trojanische Pferde die Gefahrenquelle Nummer 1 dar, dicht gefolgt von «Distributed Denial of Service Attacks» (siehe «Vorsicht Phishing-E-Mails»). Die Netz- und Informationssicherheit ist definitiv ein dynamisches Problem. Die Geschwindigkeit des technologischen Wandels bringt permanent neue Herausforderungen mit sich. Die Probleme von gestern existieren nicht mehr und

die Lösungen von heute sind morgen schon wieder wertlos. Leider genügt die Implementation von technischen Geräten wie herkömmliche Firewalls und Antivirenprogramme schon längst nicht mehr. Gefragt sind anerkannte Sicherheitsspezialisten und vor allem eine permanente Wartung sowie Weiterentwicklung. Sicherheit hört sich nicht nur teuer an, es ist tatsächlich teuer – aber für das Unternehmen unabdingbar. Eine Tatsache, welcher in Management-Kreisen leider noch zu wenig Bedeutung geschenkt wird.

Gesamtheitliche Schutzmassnahmen

Die Haltung «Wir haben ja eine Firewall ...» kann fatale Auswirkungen haben. Gefragt sind aktuelle und vor allem gesamtheitliche Schutzmassnahmen. Um ein Firmennetzwerk gegen Bedrohungen aus dem Internet abzusichern, bedarf es der so genannten «Zugangssicherheit» und der «Inhaltssicherheit». Im gesamtheitlichen Denken darf der wichtigste Teil, nämlich die «Sicherheitsdienstleistungen» nicht vernachlässigt werden. Es ist einfach, einen Benutzer zu überlisten, seine Passwörter oder Zugangscodes bekannt zu geben. Daher sind Schulungen und vor allem eine restriktive Sicherheitspolitik in Form von Richtlinien und Weisungen ein wichtiger Bestandteil der Sicherheit und gehören somit zu den umfassenden «Sicherheitsdienstleistungen». Bedenken Sie beispielsweise, dass ein Mitarbeiter Informationen über verschiedenste Kanäle wie über Telefon, Fax, Diskette, Modem als auch über Internetverbindungen und Notebooks problemlos weitergeben kann.

Unterschätztes Risiko «E-Mail»

Zweifellos bildet eine leistungsfähige Firewall-Infrastruktur und korrekte Sicherheitskonfiguration eine unabdingbare Voraussetzung. Doch es reicht nicht aus. Sie können die «beste» Zugangssicherheit in Form von teuren Firewalls haben, wenn Sie einen Virus per E-Mail erhalten und aktivieren ist es schon passiert. Zu schnell können vertrauliche Informationen aus Ihrem Firmennetzwerk nach aussen transportiert werden, denken wir einfach an vertrauliche Dokumente in Ihrer Dateiablage, die unbemerkt an hunderte



oder mehr E-Mail-Adressen versendet werden. Wenn Sie es bemerken, ist es leider definitiv zu spät. Deshalb verlangt der Betrieb eines Mail-Servers nach entsprechendem Antiviren-Schutz. «Viren-Gateways» sind Server, welche als Zwischenstation vom Internet und dem eigentlichen E-Mail-Server fungieren. So unterzieht sich jede eingehende oder ausgehende Nachricht einer zwingenden Virenkontrolle. Als wichtiger Bestandteil muss diese Zwischenstation über eine permanente Verbindung zum Produkthersteller verfügen, nur so ist eine permanente Aktualität der Virendefinitionen

und somit möglichst hohe Sicherheit gewährleistet. Diese Massnahme sorgt im Bedarfsfall für sekundenschnelle Aktualisierungen, so dass Ihr Netzwerk immer bestens geschützt wird. Für Sie und Ihre Mitarbeiter entfällt damit die Notwendigkeit zeitraubender, regelmässiger und manueller Aktualisierungen der Virusdefinitionsdateien. Solche zentralen Antivirenprodukte garantieren den ultimativen Schutz der Datenintegrität, da alle ein- und ausgehenden E-Mails noch vor Erreichen des eigentlichen Mailservers überprüft werden, was eine Virusinfektion Ihres Netzwerks wirkungsvoll verhindert.

Sicherheitslösungen für KMU

Umfassende Sicherheitsboxen eignen sich gerade für KMU, denn diese bieten auch kleinen und mittleren Unternehmen einen Rundum-Schutz auf engstem Raum zu vernünftigen Preisen. Es gibt Sicherheitsboxen, welche mit einem wegweisenden gesamtheitlichen 24x7 Managed Sicherheitskonzept überzeugen. Die Kombination einer «Internet Threat Protection Appliance» beinhaltet alle wichtigen Komponenten für einen umfassenden Netzwerkschutz: Firewall, IDP Intrusion Detection und Prevention, Anti-Virus, Anti-Spam und neu auch Anti-Phishing. Weiter sind VPN Virtual Private Networking sowie Content Filtering integriert. Wichtiger als der eigentliche Leistungsumfang bei Sicherheitsboxen ist aber die ständige Aktualität – der umfassende Sicherheitsschutz nützt wenig, wenn die Komponenten nicht aktualisiert sind. Wöchentliche, monatliche oder gar halbjährliche Aktualisierungszyklen sind längst ungenügend, heute ist die absolute Echtzeitaktualisierung notwendig. Auch hier bestreitet eine Sicherheitsbox neue Wege: Mit dem 24x7 Moni-

Intrusion Detection Systeme (IDS)

Ist diese Multifunktionalität das Non-Plus-Ultra? Unter «Intrusion» versteht man die absichtliche Verletzung der Sicherheitsmassnahmen eines Systems. Das Ziel der Intrusion Detection (ID) ist es, diese Verletzungsversuche zu erkennen und mittels Intrusion Response System (IRS) geeignete Gegenmassnahmen zu treffen, beispielsweise die Sperrung der IP-Adresse des Angreifenden oder die Alarmierung zuständiger Sicherheitsfachleute.

Intrusion-Funktionen ergänzen die Firewall in sinnvoller Weise, indem sie sämtliche Daten-Pakete einer eingehenden Analyse unterziehen und zwischen zulässigem Datenverkehr und echten Angriffen, die sowohl von innen als auch von aussen erfolgen, unterscheiden. Die ständig zunehmenden Sicherheitsbedrohungen und raffinierten Hacker-Aktivitäten verlangen moderne Systeme und Firewalls mit integriertem IDS Funktionalität. Mit Hilfe der Intrusion Detection Systeme ist es möglich, anhand von verdächtigen Aktivitäten im Netzwerk Angriffe schon im Vorfeld zu erkennen und abzuwehren.

tor- und Update-Service, eine entwickelte und patentierte «Global-Push-Technik», sorgt für eine permanente und automatische Aktualisierung von spezialisierten Operating Centers aus.

Fazit

Absolut sichere Lösungen gibt es in der Informatik nicht. Die Bedrohungen sind zu vielfältig und dynamisch. Wer es aber

schafft, die drei Lösungsansätze «Zugangssicherheit», «Inhaltssicherheit» und «Sicherheitsdienstleistungen» ideal zu einem Ganzen zu verbinden, verfügt denn auch über angemessene Informatik- und Internetsicherheit. Umfassende Sicherheitsboxen sind ein guter Ansatz, denn diese bieten die benötigte Leistung zu vernünftigen Preisen. Wichtig ist aber, dass diese Sicherheitseinrichtungen permanent aktualisiert werden. ■