Bild: stockxchng

DOSSIER SECURITY
IN KOOPERATION MIT BOLL ENGINEERING

Aber sicher!

mur. Was passiert eigentlich, wenn ein firmeneigenes Gerät verloren geht? Das Unternehmen wird sofort über den Verlust informiert, richtig? Falsch. Laut einer Umfrage des Marktforschers TNS Infratest macht das in kleineren und mittleren Unternehmen gerade mal jeder fünfte Mitarbeiter innerhalb einer Stunde. Gleichzeitig ist aber die Mehrheit der im Auftrag von Kaspersky Lab europaweit befragten IT-Entscheidungsträger davon überzeugt, dass die auf dem Gerät gespeicherten Daten über ein Passwort hinreichend geschützt sind.

Kommen also unternehmenseigene Notebooks, Tablets oder Smartphones abhanden, dauert es im Normalfall einige Stunden, bis das Unternehmen von dem Verlust erfährt und reagieren kann. In 12 Prozent aller Fälle vergeht sogar mehr als ein Tag. So lange haben Cyberkriminelle dann die Möglichkeit, von den Geräten vertrauliche Daten abzuziehen, Verträge auszuspionieren, Firmen-E-Mails zu lesen oder sich in Onlinekonten (etwa von Facebook und Twitter) einzuloggen.

Während die Zahl der IT-Geräte in Unternehmen zunimmt, sinken die Budgets der Informatikabteilungen – und somit auch das für IT-Sicherheit. Diese Konsolidierung zieht sich durch alle Firmengrössen. Wie sollen Unternehmen darauf reagieren? Und wie können CIOs ihre IT-Umgebungen trotzdem sicherhalten? Ein möglicher Ausweg ist Managed Outsourcing, wie sie zum Beispiel das Aargauer Unternehmen Seabix anbietet. Dieses Modell mache IT-Sicherheit plan- und bezahlbar, sagt CEO Thierry Kramis im in diesem Dossier – auch für kleinere Unternehmen.

Ein Fachartikel vom Sicherheitsexperten Boll Engineering erklärt zudem, wie integrale Endpoint-Security-Plattformen Cyberrisiken minimieren können. Plattformbasierte Gesamtlösungen mit einer einheitlichen Managementkonsole erhöhen die Sicherheit eines Unternehmens massgeblich. Auf dass Botnets, Viren und Trojaner in Zukunft kaum noch eine Chance haben! <

> **Seite 46**
Integrale «Endpoint Security» minimiert Cyberrisiken

> **Seite 48**
Thierry Kramis, Seabix: «ICT-Sicherheit ist bezahlbar»

Integrale «Endpoint Security» minimiert Cyberrisiken

Um Malware und hochentwickelten Angriffen firmenweit, schnell und wirksam zu begegnen, sind nicht nur Gateway-Security-Lösungen wie UTM-Appliances und Next Generation Firewalls notwendig. Auch integrale Endpoint-Security-Plattformen mit zentraler Managementkonsole optimieren die Gesamtsicherheit des Unternehmens. Jürg Hefel

Firewalls, UTM-Appliances, Next Generation Firewalls – Security-Plattformen dieser Art sind aus dem Bereich der Perimeter- beziehungsweise Gateway-Security nicht mehr wegzudenken. Sie leisten einen elementaren Beitrag zum Schutz von Netzwerk und Daten, von Applikationen und Usern. Doch ihrer Bedeutung, modernen Architekturen, leistungsfähiger Hardware und intelligenten Algorithmen zum Trotz: Gateway-Security-Lösungen allein reichen nicht aus, um einen kompletten Schutz gegen Malware und andere Bedrohungen zu gewährleisten. Notwendig ist vielmehr die gleichzeitige Einbindung einer integrativen «Endpoint Security»-Strategie. Dies namentlich aufgrund der folgenden Trends.

Raffinierte Angriffe

Die Qualität von Cyberattacken ist beeindruckend. Frühere Angriffe zeichneten sich vor allem durch eine breite Streuung von Viren und Trojanern aus. Charakteristisch waren unspezifische Attacken auf unzulänglich geschützte Informationen und Infrastrukturen. Moderne Angriffsformen sind dagegen wesentlich raffinierter und gezielter. Sie zielen auf ausgewählte Personen, Personengruppen oder Firmen, beispielsweise im Bestreben, mittels Werkspionage Marktvorteile zu erreichen, Daten zu entwenden, sich durch Angriffe auf Finanz-Applikationen zu bereichern, staatliche Stellen und wichtige Infrastrukturen zu schwächen und Industrieanlageteile zu zerstören. Die Raffinesse moderner Angriffe ist beängstigend. Dies wird etwa deutlich durch gezielte Attacken aus dem asiatischen Raum. Diese treffen weltweit führende Organisationen wie Microsoft und Apple oder Rüstungs- und Energiekonzerne sowie amerikanische Tageszeitungen ebenso wie Industrieunternehmen aus Europa und der Schweiz. Vielen Angriffen gemeinsam ist die Tatsache, dass sie für lange Zeit unbemerkt bleiben. Flame beispielsweise existiert seit langem, wurde jedoch erst im Mai 2012 offiziell entdeckt.

Die Angriffsformen und Methoden sind vielfältig: Viren, Trojaner, Botnets, webbasierte Angriffe («Drive-by-Downloads»), Social Engineering, DoS-Attacken – geradezu exorbitant ist deren Menge. Kaspersky Lab beispielsweise hat über 100 Millionen einzelne Bedrohungen in seiner Malware-Datenbank erfasst (Stand Januar 2013), erkennt täglich rund 200 000 neue Bedrohungen und weist auch für mobile Geräte bereits über 35 000 Bedrohungen aus.

Viele Programme – viel Angriffsfläche

Die Vielzahl angreifbarer Programme und Betriebssysteme beziehungsweise deren Nutzung hat selbst in kleineren Unternehmen sowie auf dem privaten Desktop grosse Dimensionen angenommen. Standen in früheren Jahren hauptsächlich Schwachstellen in Betriebssystemen von Microsoft Windows im Fokus von Cyberkriminellen, wird Schadcode heute mehrheitlich über andere Programme in die Rechner eingeschleust. Gemäss einer von Securelist.com durchgeführten Analyse sind Java und Adobe Acrobat Reader aktuell die meistgenutzten Einfallstore für Hackerangriffe.

Vielen Applikationen gemeinsam ist der Fakt, dass neue Versionen nicht automatisch installiert werden und dass notwendige Patches oft sehr lange auf sich warten lassen. Erschwerend kommt hinzu, dass es für Firmen immer schwieriger, wenn nicht gar unmöglich wird, Sicherheitslücken der zahlreich verwendeten Programme zu erkennen, zu dokumentieren und zu schliessen. Dadurch bleiben vorhandene Schwachstellen offen.

Herausforderung Mobilität

Die Nutzung (privater) mobiler Geräte im Firmenumfeld hat sich vielerorts zum Standard entwickelt und stellt die IT-Security vor komplett neue Herausforderungen. Viele Unternehmen erlauben ihren Mitarbeitenden ohne zusätzliche Sicherheitsmassnahmen, mobil aufs Firmennetzwerk zuzugreifen, Unternehmensdaten abzurufen und Daten lokal zu speichern. Ein Mobile Device Management (MDM), das auch Security-Funktionen wie Datenverschlüsselung beinhaltet, fehlt häufig.

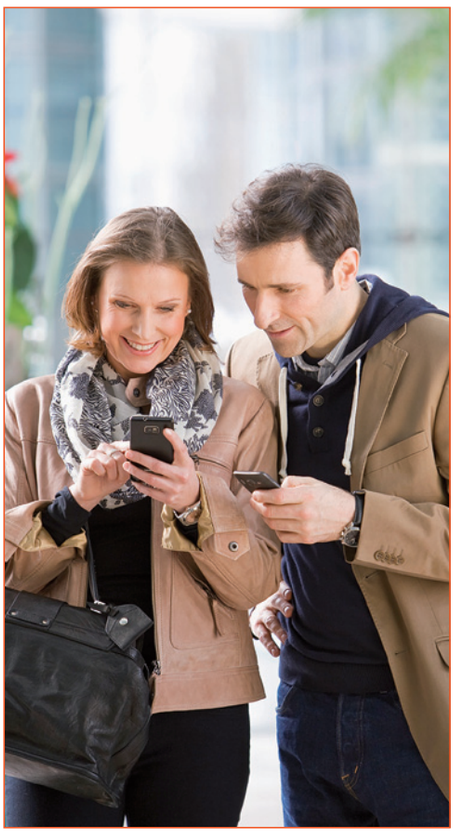
Dass mobile Geräte, die oft auch drahtlose Zugriffe auf Cloud- und Datensynchronisationsdienste ermöglichen, gerne gestohlen werden, liegt auf der Hand. Aus einer 2012 von Kaspersky Lab weltweit durchgeführten Studie geht hervor, dass bei rund 15 Prozent der befragten Firmen aufgrund gestohlener mobiler Geräte ein Datenverlust entstanden ist. Dass das (unbedarfte) Verhalten von Anwendern einen markanten Einfluss auf die Unternehmenssicherheit hat, ist unbestritten und im Bereich Social Media besonders ausgeprägt. Das Hochladen von Daten auf fremde FTP-Server etwa, das Anklicken von Adware und Umfragen, das Weiterleiten von Applikationen, die Nutzung von Diensten wie Instant Messaging und Video Streaming … diese und unzählige weitere Aktivitäten sind zur Selbstverständlichkeit geworden – ungeachtet dessen, dass sie mit hohen Risiken verbunden sind.

Von zusammengefügten Einzellösungen …

Um den vielschichtigen Bedrohungen zu begegnen, investieren Unternehmen in unterschiedlichste, sich ergänzende Tools und Technologien. So beispielsweise in Anti-Malware-Tools zum Schutz wichtiger Endpunkte, in Werkzeuge zur Verschlüsselung von E-Mails, Daten und Speichersystemen oder in Lösungen zur zentralen Verwaltung mobiler Geräte, also MDM. Auch mittels klar definierter Vorgehensweisen hinsichtlich Patch-Management – dem effizienten Verteilen und Einspielen von Software-Patches – wird versucht, Sicherheitslücken in Betriebssystemen und Programmen zu schliessen. Doch eine grosse Problematik dieses Vorgehens ist die Heterogenität der einzelnen Security-Lösungen. Diese kommunizieren nicht (oder nur spärlich) miteinander,

Jürg Hefel ist Security-Spezialist und Product Manager Kaspersky Lab bei der Boll Engineering AG in Wettingen.

erfordern eine manuelle Koordination und erschweren so die Gewährleistung einer optimalen Sicherheit. Laut dem im Januar 2013 von IDC veröffentlichten Dokument «IDC Technology Spotlight» hat die Nutzung isolierter Einzellösungen für Unternehmen und deren IT-Teams folgende Konsequenzen: mehrfache Produkteinführungen, mehrfache Update-Bereitstellung, mehrfache Skill-Sets, mehrfache Verwaltungssysteme, mehrfache Richtlinien-Engines, mehrfaches Scannen von Anwendungen und Daten.



Integrale Endpoint-Security-Plattformen ermöglichen die Kontrolle von Applikationen, Geräten und Websites und tragen somit dem sich ändernden Benutzerverhalten Rechnung. Bild: iStock

Die obige Auflistung macht deutlich: Die Komplexität, die aus der Nutzung unterschiedlichster Sicherheitslösungen entsteht, wird zum kritischen Faktor bei der Etablierung einer wirksamen Endpunkt-Security. Denn Unternehmen sind nicht – oder nur mit einem enormen Aufwand – in der Lage, die zahlreichen unterschiedlichen Systeme effizient zu verwalten, diverse Dashboards zu überwachen oder notwendige Korrekturmassnahmen zeitnah zu initiieren. Im Bewusstsein, dass der Faktor Zeit zur wirksamen Abwehr von Attacken ein Schlüsselelement ist, ist dies keine gute Nachricht. Denn das lückenlose Erkennen von und das schnelle Handeln bei Schwachstellen ist elementar. Je länger beispielsweise Programme in einer Netzwerkumgebung ohne notwendige Patches betrieben werden, umso höher ist der Gefährdungsgrad.

… zur integralen Plattform

Um den zuvor beschriebenen Problemen zu begegnen, bieten einige Endpoint-Security-Anbieter Lösungssuiten an. Diese vereinen diverse Sicherheitsfunktionen in einer Plattform, lassen jedoch eine zentrale Kontrolle vermissen. Echten Mehrwert schaffen demgegenüber integrale Gesamtlösungen, die es den Kunden erlauben, Endpunkte über eine zentrale Managementkonsole einzusehen, zu kontrollieren und zu schützen. Entsprechende Produkte zeichnen sich unter anderem durch die im Folgenden genannten Merkmale aus.

Eine Plattform – eine Konsole

Dank einer vollständig integrierten Architektur und einer umfassenden Management-Konsole lassen sich sämtliche Endgeräte (physische, virtuelle und mobile) identifizieren, kontrollieren und schützen. Da Richtlinien nur ein Mal (zentral) festgelegt werden müssen und dann per Mausklick auf mehrere Endpunkte und in verschiedenen Umgebungen verteilt werden können, wird das Sicherheitsmanagement nachhaltig vereinfacht. Zudem werden Schwachstellen plattformübergreifend und schnell erkannt und analysiert, sodass die wichtigsten Patches priorisiert und firmenweit eingespielt werden können. Darüber hinaus besteht die Möglichkeit, den Hardware- und Softwarebestand zu ermitteln und praxisrelevante Reports zu erstellen.

Ob traditionell oder cloud-basiert: Umfassende Anti-Malware- und Firewall-Funktionen wie AV, Anti-Spam und Anti-Phishing bilden die Grundlage jeder wirksamen Security-Strategie zum Schutz von Endgeräten. Mithilfe der zentralen Festlegung und Durchsetzung von Sicherheitsrichtlinien lassen sich unter anderem Berechtigungen, unterstützte Peripheriegeräte, Webzugriffe oder die Nutzung von Social-Media-Plattformen komfortabel steuern und kontrollieren. Funktionen wie «Application Control» (Zulassen, Blockieren und Steuern einzelner Anwendungen) und «dynamisches Whitelisting» sind wichtige Bestandteile einer sicherheitsorientierten Endpoint-Kontrolle.

Umfassender Schutz von Mobilgeräten

Mittels eines zentralen MDM lassen sich mobile Endgeräte – ob privat oder in Firmenbesitz – komfortabel einbinden, sichern und verwalten. Auch Daten, die sich auf Smartphones oder Tablets befinden, können wirksam geschützt werden. So etwa durch Verschlüsselung oder Löschen via Fernzugriff. Zu den weiteren typischen MDM-Möglichkeiten gehören Funktionen wie Geräte-Ortung via GPS, Sperren per Remote-Zugriff, Konfiguration und Deployment mittels E-Mails oder Thetherings, Durchsetzung von Einstellungen, Richtlinien und Zugriffsbeschränkungen etc. Bedeutsam ist in diesem Zusammenhang die Containerbildung, die eine «Zweiteilung» mobiler Geräte ermöglicht. Dadurch lassen sich private und firmeneigene Applikationen auf demselben Gerät logisch trennen und separat verwalten. So ist es einem Unternehmen beispielsweise möglich, im «Firmencontainer» des privaten Smartphones eines Mitarbeitenden die Installation von Applikationen zu erzwingen oder via Remote-Zugriff zu löschen, derweil der private Bereich in der alleinigen Kontrolle des Mitarbeitenden bleibt. Ob einzelne Dateien oder der gesamte Datenträger: Die Verschlüsselung gespeicherter Daten sorgt dafür, dass beim Verlust eines Endgeräts keine Daten in fremde Hände gelangen.

Zeitnahes Patch-Management

Hochentwickelte Schwachstellen-Scans sowie ein umfassendes Patch-Management dienen dazu, Sicherheitsrisiken zu erkennen, die notwendigen Massnahmen zeitnah zu initiieren, benötigte Patches sofort und automatisch zu verteilen und die Wirksamkeit der ausgeführten Massnahmen zu kontrollieren. Ob die Installation von Betriebssystemen, das vollautomatische Ausrollen neuer Softwareversionen oder die Verwaltung von Hardware, Software und Lizenzen … zeitraubende Aufgaben dieser Art lassen sich mithilfe einer integralen Systemverwaltung effizient und umfassend lösen.

Komplexe Sicherheitsstrategie

Die vorgenannte, nicht abschliessende Auflistung von Leistungsmerkmalen, die zur Etablierung einer umfassenden Endpoint-Security notwendig sind, macht die Komplexität einer entsprechenden Sicherheitsstrategie deutlich. Um gezielten, hochentwickelten Angriffen firmenweit, schnell und wirksam begegnen zu können, sind plattformbasierte Gesamtlösungen mit einer einheitlichen Managementkonsole unabdingbar. Sie optimieren die Gesamtsicherheit des Unternehmens, reduzieren den Verwaltungsaufwand und minimieren die Kosten. Und sie tragen dazu bei, dass Trends wie Cloud Computing und Mobilität die IT-Security nicht negativ beeinflussen und dass auch Firmen mit begrenzten Budgets von einer ganzheitlichen Security-Lösung profitieren. <

«ICT-Sicherheit ist bezahlbar»

Das Schweizer Unternehmen Seabix mit Sitz im Aargau verkauft modulare ICT-Lösungen und hat rund 5000 Kunden. Die Sicherheit der Informatik ist dabei zentral. Die Netzwoche hat bei CEO Thierry Kramis nachgefragt, welchen Stellenwert ICT-Sicherheit bei Schweizer Unternehmen einnimmt. Interview: Marcel Urech

Herr Kramis, was hat ICT-Sicherheit in Schweizer Unternehmen für einen Stellenwert?
Bei Schweizer Unternehmen nimmt die IT-Sicherheit grundsätzlich einen hohen Stellenwert ein, wird aber von externen Faktoren massgeblich beeinflusst. Sicherheit muss Kernbestandteil jeder ICT-Lösung sein. Daher gilt es in einer ersten Phase, für den Kunden eine Kostentransparenz im Bereich der gesamten ICT zu erstellen. Dadurch wird auch der Anteil der Security am Gesamtbudget der ICT sichtbar. Diese Kosten stehen in der Folge im Kontext des wirtschaftlichen Umfelds, um nur einen Faktor zu nennen. Je düsterer die wirtschaftlichen Aussichten der Unternehmen sind, desto höher ist der Druck, bei allen Kostenbereichen einzusparen – auch bei der Sicherheit. Das ist gefährlich, da potenzielle Schadensfälle in diesem Bereich ein Unternehmen nachhaltig gefährden können.

Gibt es Risiken, die von Schweizer Unternehmen systematisch unterschätzt werden?
Das Problem der ICT besteht darin, dass die Komplexität ständig zunimmt. Demgegenüber steht der Trend, dass Unternehmen, insbesondere im KMU-Markt, nur sehr beschränkt Zeit in die Analyse und das Verständnis einzelner Themenfelder, wie eben ICT-Sicherheit, investieren können. Insbesondere bei Themen, die in die ICT überführt werden, wie zum Beispiel Voice over IP wird oft vergessen, dass die Telefongespräche damit neu über Datennetzwerke funktionieren, was sie von aussen angreifbar macht. Damit fehlen oft elementare und einfach zu implementierende Sicherheitsvorkehrungen. Das ist problematisch.

Was kann das für Folgen haben?
Leider sind Angriffe auf ICT-Infrastrukturen allgegenwärtig. Das Argument, dass eine Firma zu klein oder zu unbekannt ist, um angegriffen zu werden, greift daher nicht. Die Folgen können gravierend sein. Nehmen wir noch einmal das Beispiel von Voice over IP, kurz VoIP. Es gibt zahlreiche uns bekannte Fälle von VoIP-Projekten, die den Faktor


Thierry Kramis, CEO von Seabix

Sicherheit zu wenig einkalkuliert haben. Angreifer haben dies konsequent ausgenutzt und diesen Unternehmen Schaden in der Höhe von mehreren hunderttausend Franken zugefügt. Nach einem solchen Vorfall relativieren sich die Kosten für ICT-Sicherheit beträchtlich.

Gibt es weitere solche Beispiele?
Ja, die gibt es. Um zwei konkrete Beispiele zu nennen: Kunden mit offenen Mailservern, die vom Telekommunikationsanbieter in der Folge mehrere Tage gesperrt werden, und Kunden, die ihre Daten wegen mangelndem Offsite-Back-up komplett verlieren und mehrere Wochen bis Monate nicht arbeiten können, erleiden dadurch einen grossen finanziellen Schaden.

Was kostet es, um solche Schadensfälle zu vermeiden?
Das ist von Fall zu Fall verschieden und hängt von mehreren Faktoren ab. Generell lässt sich aber sagen, dass die Kosten im Schadensfall um ein Vielfaches höher sind als die Investition in eine Sicherheitslösung. Ausserdem müssen auch die Anbieter von ICT-Systemen einen Weg finden, um die Kosten transparent darzustellen. Sie tragen ebenfalls eine Mitverantwortung, um das Thema ICT-Sicherheit beim Kunden zu etablieren. Um dem Rechnung zu tragen, betreiben wir bei Seabix die Kundeninfrastruktur im monatlichen Abo. So werden die initialen Kosten, und damit die Hürde der Anschaffung, massgeblich reduziert. In der Betriebsphase können die Unternehmen zudem die laufenden Kosten transparent budgetieren, das ist insbesondere im schwierigen Marktumfeld massgebend.

Beim Thema Sicherheit spielt auch immer der Faktor «Mensch» eine Rolle. Wie können Unternehmen diesen bändigen?
Das ist tatsächlich schwierig, da der Mitarbeiter im Unternehmen massgeblich an seiner Produktivität gemessen wird. Sicherheitssysteme werden dabei nicht immer als förderlich aufgefasst. Die Rollenverteilung der Umsetzung von ICT-Sicherheit in Unternehmen ist dabei klar. Es ist Aufgabe der technischen Entwicklung, Sicherheitssysteme so weiterzuentwickeln, dass sie dem Faktor Mensch Rechnung tragen. Es ist Aufgabe der Unternehmen ICT-Sicherheits-Policies zu definieren und umzusetzen. Dabei müssen sie beim Mitarbeiter das entsprechende Bewusstsein für die Thematik etablieren und ihm die richtigen Tools in die Hände geben. Letztlich ist es Aufgabe der ICT-Anbieter, dies transparent und korrekt umzusetzen.

Wie hat sich die Nachfrage der Kunden nach ICT-Sicherheit in den letzten Jahren verändert?
Die hohe Zahl von Vorfällen im ICT-Sicherheitsbereich stimuliert die Nachfrage. Die rechtlichen Rahmenbedingungen in der Schweiz wirken sich dabei ebenfalls positiv bei Schweizer KMUs und ausländischen Unternehmen mit Sitz in der Schweiz aus. Im Schweizer KMU-Markt arbeiten wir kontinuierlich und intensiv daran, das Bewusstsein für das Thema weiter zu schärfen. Dies schafft unseren Kunden dank tieferer Schadensfälle einen deutlichen Mehrwert zu bezahlbaren Kosten. <