Publication: netzguide (CH)
Publishing House: Netzmedien AG
Publication date: 10.02.2010
Page: 36-37

Was tun, wenn Mobile Security zum Thema wird?

Sind Mobilgeräte wirklich die neue Schwachstelle, wenn es um den Schutz von Informationen ausserhalb der Unternehmensnetzwerke geht? Cyberkriminelle rüsten auf und nutzen neue Technologien für ihre Angriffe. Und wie halten Unternehmen Schritt? Franz Kaiser

Franz Kaiser
ist Country Manager Austria, Switzerland and Central Eastern Europe bei Fortinet
fkaiser@fortinet.com

Durch den zunehmenden Gebrauch mobiler Anwendungen wie Facebook und Twitter können Mitarbeiter Unternehmensnetzwerken schaden, ohne es zu wissen. Welche Best Practices sind bei mobilen Anwendungen zu beachten und was müssen Unternehmen und Security-Fachleute über unvorhersehbare Sicherheitsfragen im Zusammenhang mit schnurlosen Geräten wissen?

Bislang hielten sich Malware-Aktivitäten bei mobilen Endgeräten wie Smartphones noch im Rahmen. Dennoch häufen sich die Anzeichen, dass dies bald ein Ende hat. Unternehmen werden anfangen müssen, sich über eine Strategie zur Abwehr mobiler Bedrohungen ernsthaft Gedanken zu machen, um sicherzustellen, dass ihre Netzwerke vor Bedrohungen aus der mobilen Kommunikation geschützt sind.

Risikofaktor 3G

Die zunehmende Verbreitung von 3G-Netzwerken - also Netzwerke für Mobilfunkleistungen der dritten Generation mit dem UMTS-Standard für Datenraten bis 7,2 MBit/s - liefern mehr Bandbreite für mobile Geräte. Doch damit wird auch verstärkt gefährlicher Datenverkehr in die Netzwerke eingeschleust. Zudem bietet 3G Netzwerkanbietern die Möglichkeit, eine grössere Bandbreite an fortgeschrittenen, mobilen Services wie Echtzeitzugriff auf High-Quality-Audio- und -Video-Übertragungen bereitzustellen. Apple, ein vergleichsweise kleiner Player im Handset-Markt, hat mit seinem Applikationsportal bereits die Art und Weise beeinflusst, wie Nutzer mit ihren Smartphones interagieren. Microsoft und Nokia ziehen mit ähnlichen Portalen nach. Die verstärkte Personalisierung und Kundenanpassung, die mit diesen Portalen möglich wird, bringt allerdings neue Anwendungsmöglichkeiten der Portale - gute wie schlechte - mit sich. Das ist auch die grosse Sorge der Manager von Unternehmensnetzwerken. Durch

die neuen Applikationen sind Nutzer nicht länger an vorinstallierte Applikationen gebunden. Darüber hinaus nutzen Verbraucher ihre Smartphones immer mehr für geschäftliche wie auch persönliche Zwecke. Das US-Marktforschungsunternehmen iSuppli prognostizierte im März 2009, dass die Anzahl an ausgelieferten Smartphones im letzten Jahr eine Höhe von 192,3 Millionen Stück erreichen wird. Das sind 11,1 Prozent mehr als noch im Vorjahr.

Smartphones als neue Bedrohung für die Unternehmenssicherheit

Verbraucher personalisieren ihre Smartphones nicht nur mehr und mehr, die Mobilfunkgeräte werden für Nutzer auch immer unentbehrlicher. Das heisst im Klartext: Kunden geben dafür Geld aus - und wo Geld im Spiel ist, lässt auch die Kriminalität nicht lange auf sich warten. Das Potenzial für Vireninfektionen und Angriffe steigt drastisch an. Smartphones stellen dabei einen immer grösser werdenden Risikofaktor dar. Aufgrund ihrer Fähigkeit des Echtzeitzugriffs auf Unternehmensnetzwerke werden sie verstärkt als mobiles Büro genutzt, so wie es früher bei Laptops der Fall war. Für Cyberkriminelle eröffnet sich hier die Möglichkeit, Smartphones als Ausgangspunkt für den Zugriff auf sensible Unternehmensdaten zu nutzen. Somit kann in der verstärkten Verwendung von Smartphones und anderer schnurloser Geräte sowie dem Einsatz neuer Businessmodelle die grösste Bedrohung für die Sicherheit in Unternehmen in nächster Zeit gesehen werden.

Integrierte End-to-End-Netzwerk-Security-Plattform als ideale Lösung

Im Gegensatz zum traditionellen PC-Markt nimmt der Mobilfunkmarkt eine spezielle Position ein, wenn es um Malware geht. Während für Angriffe auf Desktops und Laptops mit Windows, Mac und Linux nur eine begrenzte Anzahl an Plattformen zur Verfügung steht, steigt die Anzahl mobiler Plattformen mit Google, Android, Apple Mobile OS, SymbianOS, Windows Mobile und Palm. Die Schwachstelle im Google Android OS, die Ende 2008 entdeckt wurde, stellt dabei nur die Spitze des Eisbergs dar. Und der mobile Wurm «Sexy View», der im Februar 2009 Schaden anrichtete, weist stark darauf hin, dass wir uns am Wendepunkt zu einem mobilen Botnetz befinden. Die ausgeklügelte Strategie der Verbreitung via SMS, bei der der Wurm auf bösartigen Servern gehalten wird, erlaubt es Cyberkriminellen nämlich, den Wurm immer wieder erfolgreich zu verändern und Funktionalitäten hinzuzufügen oder zu eliminieren.

Zum Schutz mobiler Endgeräte bedarf es eines gemanagten Clients, der Softwareinstallationen aufdecken und den Dateizugriff überwachen sowie zusätzlich Daten verschlüsseln und Statusmeldungen an einen zentralen Server übermitteln kann. Netzwerkmanager werden Lösungen benötigen, die vielschichtigen Schutz vor sogenannten «Blended Threats» bieten und alle Schnittstellen an Endgeräten absichern können. Die ideale Lösung für mobile Clients ist daher eine integrierte End-to-End-Netzwerk-Security-Plattform mit beschleunigter Hardware und minimalen Performanceeinbussen für Endgeräte und Verbraucherdienste. Darüber hinaus sollte diese Netzwerk-Security-Plattform Konfigurationsmanagement und -kontrolle durch spezielle Reportingmöglichkeiten bieten sowie die Erstellung flexibel definierbarer Profile und Richtlinien für eine granulare Netzwerksegmentierung ermöglichen.

Mit steigender Verwendung mobiler Applikationen entdecken auch Cyberkriminelle zunehmend einen neuen, lukrativen Bereich für sich. Bildquelle Fotolia, Montage Netzwoche

Jailbreak für Handys als aktuelle Schwachstelle Nummer eins

Viele Verbraucher nutzen mittlerweile Mobiltelefone mit Jailbreak wie zum Beispiel das iPhone. Das bedeutet, die Telefone werden für die Installation von Fremdsoftware geöffnet, was ein erhebliches Sicherheitsrisiko darstellt. Beim iPhone lassen sich mit einem solchen Jailbreak beispielsweise das iPhone der ersten Generation und das iPhone 3G auf die Firmware 3.0 aktualisieren und zudem für andere Software öffnen, die nicht im offiziellen AppStore von Apple verfügbar ist. Verbraucher sollten sich derartiger Risiken unbedingt bewusst sein, wenn sie Funktionalitäten ihrer Mobiltelefone freischalten. Denn wie gefährdet Mobiltelefone mit Jailbreak sind, zeigt ein aktueller Wurm, der es auf Apple iPhones mit Jailbreak abgesehen hat. Erst vor einigen Wochen tauchte der erste Wurm für das iPhone auf. Damals handelte es sich allerdings noch um eine ungefährliche Demonstration, die nur auf die Sicherheitslücke hinweisen sollte, die durch einen Jailbreak entstehen kann. Der neue Wurm nutzt offenbar genau diese Lücke, um sich Zugriff auf Daten zu verschaffen, die auf dem Telefon gespeichert sind. Zudem soll der Schädling von einem iPhone aus weitere Apple-Handys scannen und sich auch dort Zugang verschaffen.

Beobachtet man die Entwicklungen im Mobilfunkmarkt, so ist eine deutliche Tendenz zu erkennen: Mit der steigenden Verwendung mobiler Applikationen entdecken auch Cyberkriminelle zunehmend einen neuen, lukrativen Bereich für sich. Der Security-Markt wie auch Unternehmen werden auf diese Entwicklungen schnell reagieren müssen, um für diese neue Welle der Cyberkriminalität gewappnet zu sein.