Link: https://www.computerwoche.de/a/sicherheitsrisiko-iphone-und-co,1880517

IT-Security

Sicherheitsrisiko iPhone & Co.

Datum: 08.12.2008
Autor(en): Oliver Häußler

Spätestens seit nun auch das iPhone neben BlackBerry, Notebook oder Smartphone im beruflichen Umfeld eingesetzt wird, steht der mobile Mitarbeiter wieder im Rampenlicht der IT-Sicherheit: So attraktiv mobile Endgeräte auch sein mögen, aus der Perspektive der Netzsicherheit stellen sie eine Sicherheitslücke im System dar.

Für Manager sind sie Spielzeug, Statussymbol und unentbehrliches Equipment im **beruflichen**[1] wie auch im privaten Umfeld. Den IT-Sicherheits-Verantwortlichen dagegen bereiten sie schlaflose Nächte - die Rede ist von **Mobile Devices**[2], die in Form von **PDAs, BlackBerrys, Notebooks, Laptops oder Smartphones**[3] immer häufiger im Unternehmen eingesetzt werden.

Speziell das **iPhone**[4] und der **BlackBerry**[5] bezaubern die Anwender durch Funktionalität gleichermaßen wie durch ihr attraktives Design. Die Folge: Der Einsatz dieser Endgeräte wird nicht allein auf das Unternehmen begrenzt. Durch die zusätzliche private Nutzung entsteht eine neue **Sicherheitslücke**[6].

Wer beim Einsatz mobiler Geräte keine Sicherheitsvorkehrungen trifft riskiert nicht nur Angriffe auf sein Netzwerk, sondern gefährdet unter Umständen das gesamte Unternehmen.

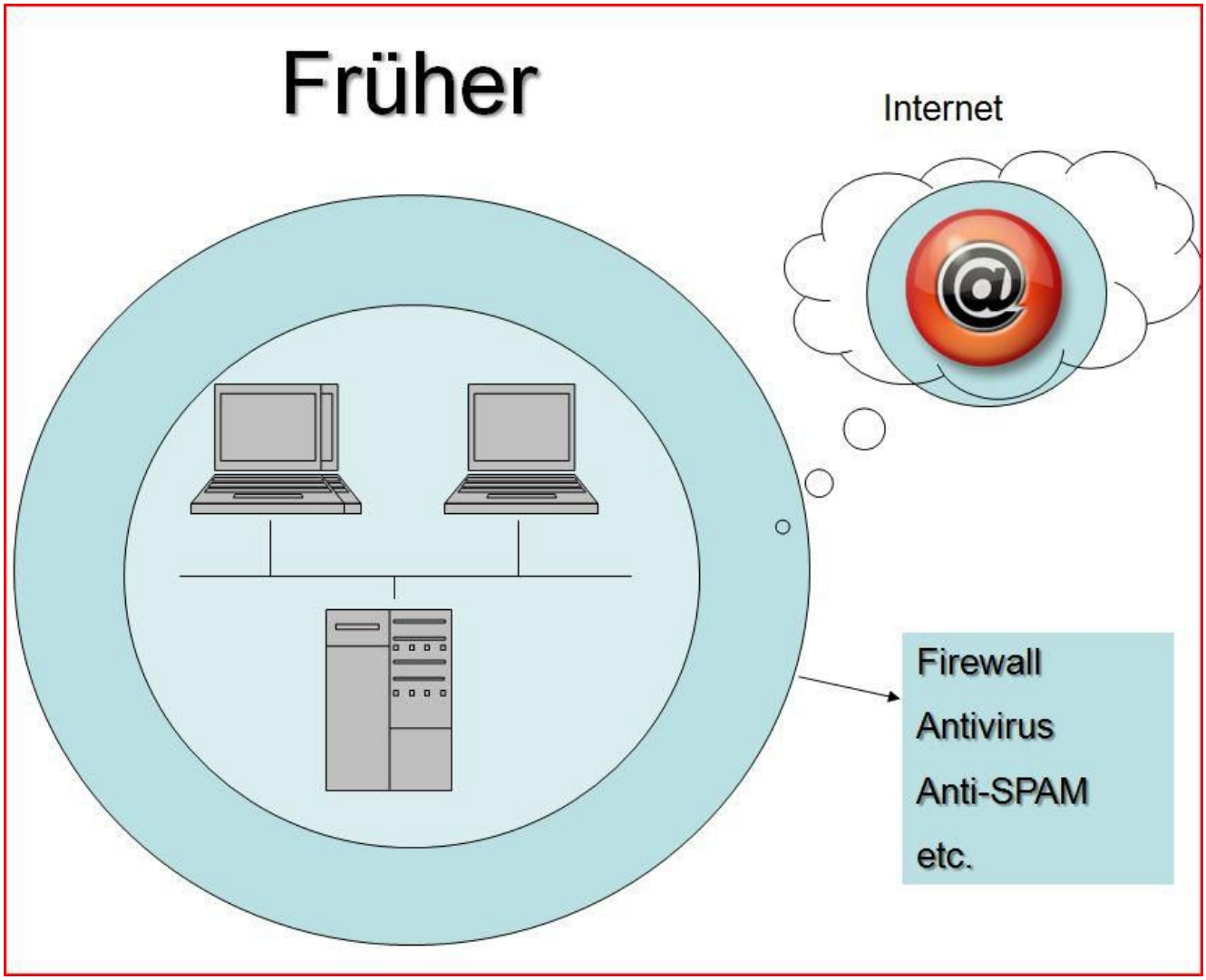
Der neue Trend: "Web-to-go"

Trend zur Mobilität: Die steigende Anzahl mobiler Mitarbeiter stellt neue Anforderungen an die Kommunikation.

Markttreiber für diese Entwicklung ist der zunehmende Wunsch nach mehr Mobilität, die sich durch **konvergente Mobilfunknetze**[7] und leistungsstarke Endgeräte immer komfortabler gestalten lässt. Nach dem Handy-Telefonieren und der mobilen E-Mailanwendung zeichnet sich die Nutzung mobiler Internet-Angebote schon heute als nächster Trend ab: "Mit über zehn Millionen Nutzern hat Mobile Internet in Deutschland den Durchbruch geschafft", lautet das Ergebnis einer **Studie zur Zukunft des mobilen Internets von Deloitte**[8]. Wegen der aktuell noch einseitigen E-Mailnutzung wollen die Marktbeobachter zwar derzeit nicht von einem wirklichen Massenmarkt sprechen. Sie gehen jedoch davon aus, dass bei einer endgültigen Marktdurchdringung des **3G-Standards**[9] bei Mobilfunkgeräten die "Nutzer so selbstverständlich wie heute über stationäre Computer in absehbarer Zukunft mit mobilen Endgeräten im Web surfen und E-Mails schreiben." Bis Ende 2012 erwarten Experten eine Verdopplung der heutigen Nutzerzahlen.

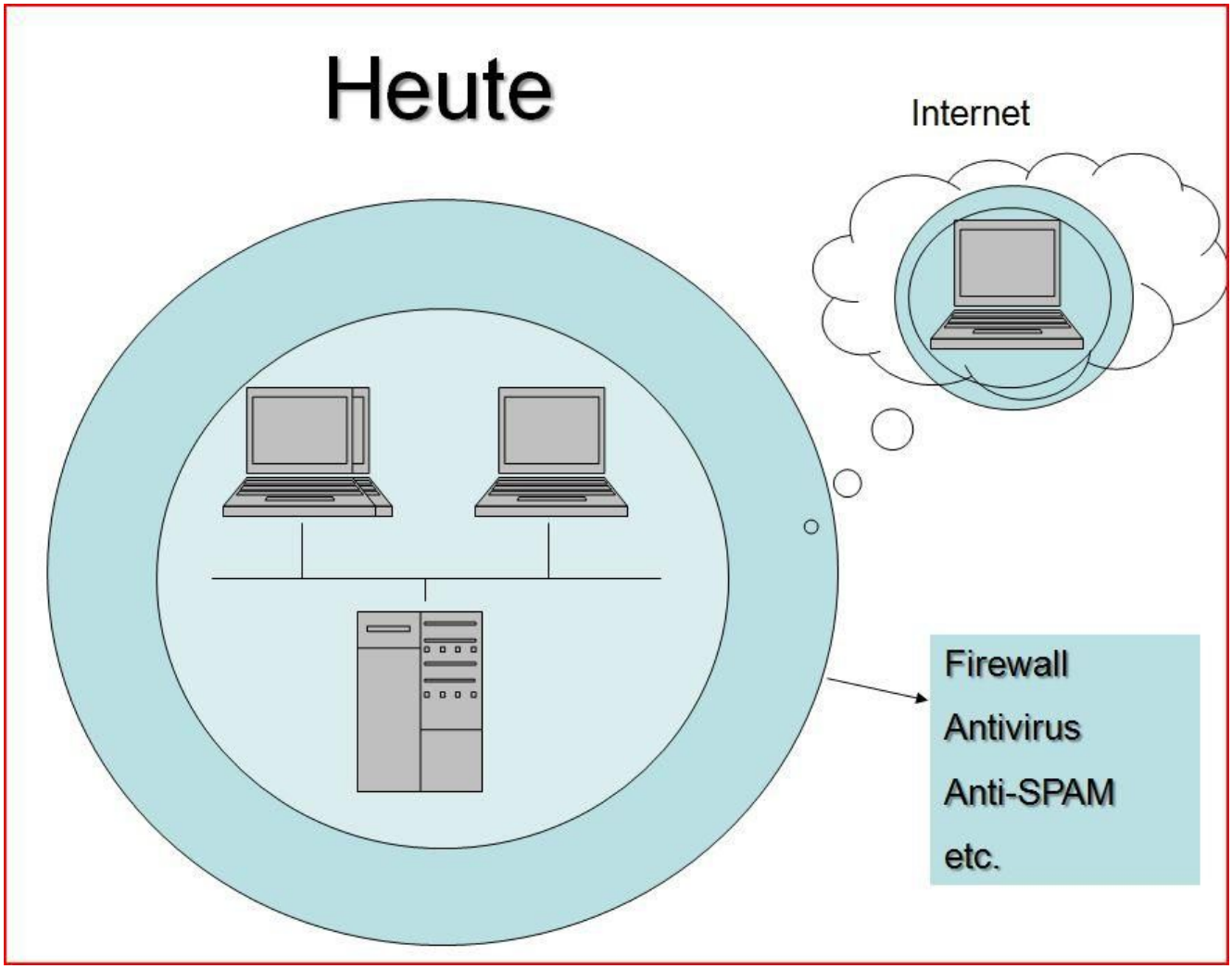
An der Firewall vorbei

Sicherheitsverantwortlichen und IT-Administratoren bereitet dieser Trend Kopfschmerzen. Wählt sich der Anwender mit seinem mobilen Endgerät auch außerhalb des geschützten und überwachten Netzwerk-Sicherheitssystems ins Internet ein, kann sich schnell ein Virus oder Wurm darauf einnisten. Zurück im Unternehmen wird das Gerät wieder ins Netz eingeloggt und die Malware hat freie Bahn, um sich im gesamten System auszubreiten. Steht ein solches Einfallstor offen, wird die beste Firewall wirkungslos.



Netzwerksicherheit früher: Abgeschlossene Systeme waren einfach abzusichern.

Die größte Sicherheitslücke stellen derzeit **Notebooks und Laptops**[10] dar, da mobile Mitarbeiter häufig zwischen den Arbeiten im Firmennetz und außerhalb wechseln. Um die Gefahr von Viren und anderen Bedrohungen abzuwenden, sind **Sicherheitsvorkehrungen**[11] an den Geräten vorzunehmen. Dazu gibt es verschiedene Möglichkeiten: Am sichersten ist es, das Betriebssystem doppelt auf zwei unterschiedlichen Partitionen zu installieren - ein System für den LAN-Betrieb, das andere für den externen Einsatz. Das trennt die beiden Bereiche komplett voneinander und ein Virus von außerhalb könnte nicht nach innen gelangen. Allerdings ist diese Variante für den Anwender nicht besonders attraktiv, da er in den häufigsten Fällen auf ein und dieselben Dateien von seinen unterschiedlichen Standorten aus zugreifen will. Er müsste sich die bearbeiteten Dokumente über den Umweg E-Mail ins Netz schicken, um sie auf dem anderen Betriebssystem weiter zu verwenden. Das ist nicht komfortabel und macht die Arbeit komplizierter, nicht zuletzt, weil dann auch unterschiedliche Dateiversionen entstehen.



Netzwerksicherheit heute: Mobile Endgeräte erfordern zusätztliche Maßnahmen zur Absicherung der Netzwerke.

Maßnahmen zur Absicherung

Der Sicherheitsexperte des Online-Portals **tecchannel**[12], Mike Hartmann, empfiehlt: "Die wichtigste Maßnahme besteht darin, dass die aktuellsten Sicherheits-Patches für Windows und den Internet Explorer eingespielt werden, und zwar am besten, ohne dass der Benutzer eingreifen muss oder darf." Hilfreich sei es, den Software-Update-Service im LAN einzurichten.

Außerdem sollte der lokale Benutzer des Notebooks nicht als Hauptbenutzer eingetragen sein. Hartmann: "Für den Internet Explorer richten Sie die erlaubten ActiveX-Controls wie beispielsweise Flash oder Netmeeting vorab ein und sperren dann den Download weiterer Controls per Group Policy Editor (gpedit.msc)". Prinzipiell sollten alle **Sicherheitseinstellungen**[13] vom Administrator vorgenommen werden. Die Rechte des Nutzers, Änderungen an den Sicherheitseinstellungen vorzunehmen, sind dagegen zu begrenzen.

Hartmann empfiehlt weiterhin Tools wie **Spybot Search&Destroy**[14] zur weiteren Absicherung des Internetexplorers. "Die Funktion ´Immunisieren´ sperrt beispielsweise als gefährlich erkannte ActiveX-Controls. Und über die Hosts-Datei können Sie den Zugriff auf potenziell gefährliche oder unerwünschte Websites verhindern."

Wichtig sei darüber hinaus die Installation eines Virenscanners auf dem Notebook und das Abschalten einer Reihe von Diensten, die unter Windows gestartet werden, "die teilweise überflüssig sind und teilweise sogar die Sicherheit gefährden, wenn sie auf einem Rechner laufen, der ungeschützt mit dem Internet verbunden ist". Dazu zählen beispielsweise der Nachrichten- oder der Serverdienst.

Empfehlenswert seien darüber hinaus lokale Firewalls für die Geräte, vor allem wenn sie über ungesicherte Zugänge eine Verbindung zum Internet aufbauen.

Alle systemtechnischen Maßnahmen sind jedoch wirkungslos, wenn die Anwender nicht dafür sensibilisiert und geschult werden. Hartmann empfiehlt, Verhaltensmaßregeln und Anleitungen für das mobile Surfen im Internet aufzustellen und die Mitarbeiter darüber zu informieren.

Generell sollten mobile Geräte stets mit starken Passwörtern gesichert werden. Bei **Verlust oder Diebstahl**[15] könnten sämtliche Daten in falsche Hände geraten. Hat das Notebook eine VPN-Verbindung zum Internet, greift der Dieb auch auf Unternehmensdaten zu. Schützenswerte Daten auf dem mobilen Gerät sind zusätzlich zu verschlüsseln.

Ergänzend zu den Maßnahmen am Endgerät sind auch Vorkehrungen im Netzwerk zu treffen. Hartmann: "Der erste Schritt sollte sein, das Paradigma ´Wer im LAN ist, dem vertrauen wir´ zu den Akten zu legen. Wenn Ihre Infrastruktur beispielsweise VLANs unterstützt, können Sie alle Notebooks in einem separaten Netz sammeln, das durch ein Security-Gateway vom normalen LAN abgekoppelt ist". Weitere Sicherheitsmaßnahmen bieten Verfahren wie **NAC (Network Admission Control, Network Access Control)**[16] und **NAP (Network Access Protection)**[17].

iPhone in der Kritik

Anlass für Sicherheitsdiskussionen bietet seit seiner Einführung das **iPhone von Apple, das inzwischen auch vielfach im Unternehmen eingesetzt**[18] wird. "Die sichere Speicherung von Informationen auf dem Gerät ist nur begrenzt möglich", fasst ein Report von **Berlecon Research in Kooperation mit Fraunhofer ESK**[19] zusammen. Dies zeige sich daran, dass "Unternehmen, die mit signierten und/oder verschlüsselten E-Mails kommunizieren, das iPhone 2.0 nicht einsetzen können. Unverschlüsselte E-Mails sowie Dateianhänge liegen aufgrund der nicht vorhandenen Datenverschlüsselung im Klartext vor".

Doch damit nicht genug: "Sehen unternehmensinterne Richtlinien die Verwendung eines Zugangspassworts bei mobilen Endgeräten vor, so kann das iPhone 2.0 nur unter der Bedingung eingesetzt werden, dass Benutzern die Abschaltung des Zugangsschutzes untersagt wird - technisch kann diese Vorgabe nicht gewährleistet werden," so der Report weiter.

Die Verfasser des Berichts raten zum Einsatz zusätzlicher Applikationen, die fehlende Sicherheitsmechanismen wie die Verschlüsselung von E-Mails nachbilden.

Lösungen für kleine Unternehmen

Vor allem kleine und mittelständische Betriebe haben nicht die Ressourcen für eine aufwändige Geräte- und Netzwerkabsicherungen. Geht es Ihnen in der Anwendung lediglich um die nahtlosen **Mobilfunk- und Festnetzintegration**[20], so eignen sich Angebote wie beispielsweise der **Octopus Mobility Services**[21] von **T-Systems**[22]. Diese Systeme haben die mobilen Endgeräte auch in puncto Sicherheit abgestimmt. Doch auf für die **mobile Einwahl ins Firmennetz**[23] und für **mobile Internetzugänge**[24] gibt es sichere Lösungen auf dem Markt, die dem Anwender einen hohen Komfort bieten und dem IT-Administrator die Sorgen - und hoffentlich auch die Kopfschmerzen um die IT-Sicherheit - nehmen.

Links im Artikel:

[1] **https://www.computerwoche.de/job_karriere/arbeitsmarkt/1877447/index8.html**
[2] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1865059/**
[3] **http://www.mittelstand.t-systems.de/tsi/de/425800/Home/Mittelstand/Produkte-und-Loesungen/Mobilitaet/Mobilfunk-und-Festnetzintegration/Octopus-Mobility-Services/1-octopus-mobility-services**

[4] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1874485/**
[5] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1868182/**
[6] **https://www.computerwoche.de/knowledge_center/mobile_wireless/1873404/**
[7] **https://www.computerwoche.de/knowledge_center/netzwerke/1870656/**
[8] **http://www.deloitte.com/dtt/research/0%2C1015%2Ccid%3D228922%2C00.html**
[9] **http://en.wikipedia.org/wiki/3G**
[10] **https://www.computerwoche.de/knowledge_center/security/582662/**
[11] **https://www.computerwoche.de/knowledge_center/notebook_pc/1873722/**
[12] **https://www.tecchannel.de/**
[13] **https://www.computerwoche.de/knowledge_center/security/1874650/**
[14] **https://www.computerwoche.de/knowledge_center/security/448445/index4.html**
[15] **https://www.computerwoche.de/knowledge_center/it_security/1855169/**
[16] **http://de.wikipedia.org/wiki/Network_Access_Control**
[17] **https://www.tecchannel.de/link.cfm?pk=462287**
[18] **https://www.computerwoche.de/subnet/t-systems/1878011/**
[19] **http://www.berlecon.de/iphone**
[20] **http://www.mittelstand.t-systems.de/tsi/de/425800/Home/Mittelstand/Produkte-und-Loesungen/Mobilitaet/Mobilfunk-und-Festnetzintegration/Octopus-Mobility-Services/1-octopus-mobility-services**
[21] **http://www.mittelstand.t-systems.de/tsi/de/425800/Home/Mittelstand/Produkte-und-Loesungen/Mobilitaet/Mobilfunk-und-Festnetzintegration/Octopus-Mobility-Services/1-octopus-mobility-services**
[22] **http://www.etracker.de/rdirect.php?et=mNmDKb&et_cid=11&et_lid=107&et_url=http://mittelstand.t-systems.de/tsi/de/508540&et_sub=DE-computerwoche**
[23] **http://www.mittelstand.t-systems.de/tsi/de/429466/Home/Mittelstand/Produkte-und-Loesungen/Vernetzung-und-VPN/Mobile-Einwahl-ins-Firmennetz**
[24] **http://www.mittelstand.t-systems.de/tsi/de/429518/Home/Mittelstand/Produkte-und-Loesungen/Mobilitaet/Mobile-Internetzugaenge**
