IT-SECURITY

Sicherheits-Richtlinien für Endgeräte

Jede Woche beantworten Sicherheitsexperten Leserfragen und geben Ratschläge, wie sich die Sicherheit in einem Unternehmen erhöhen lässt.

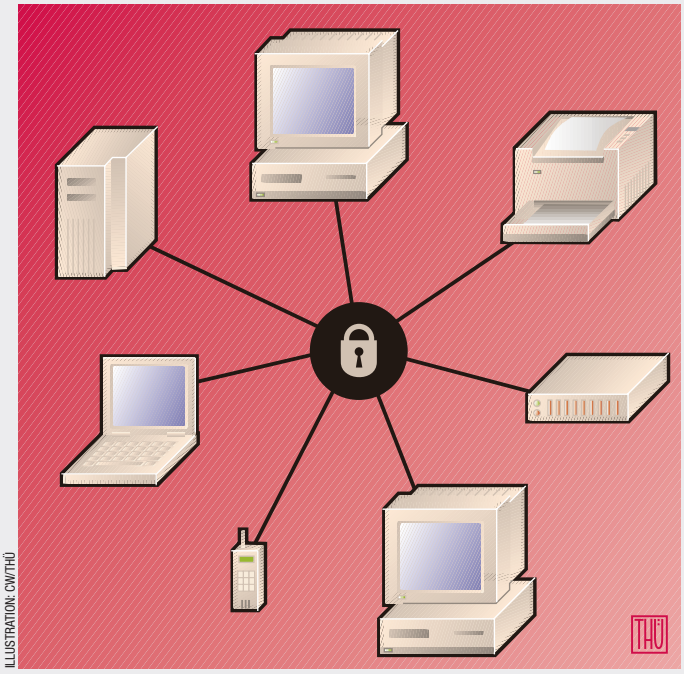

ILLUSTRATION: CW/THÜ

Frage: Heute werden mannigfaltige Endgeräte wie Desktop-PC, Drucker, Wireless Notebooks und PDA für die firmeninterne Kommunikation eingesetzt. Lässt sich überhaupt bei dieser Vielfalt eine sichere Kommunikation erreichen ?

In der Tat sehen sich die Sicherheitsverantwortlichen mit einer breiten Palette untereinander kommunizierender Systeme konfrontiert. Oft sind diese Systeme von unterschiedlichen Herstellern produziert und auch ihre Einsatzgebiete sind äusserst individuell. Vom klassischen Desktop-PC, eventuell mit verschiedenen Betriebssystemen, über netzwerkfähige Drucker bis hin zum drahtlosen Notebook oder PDA (Personal Digital Assistant) wird in modernen Unternehmungen oft alles verwendet. Die firmeninternen, drahtgebundenen Systeme sind meist gut gesichert und kontrolliert. Doch wie steht es um die Sicherheit der extern verwendeten Notebooks? Und wie sicher sind eigentlich die Systeme von Partnern, Lieferanten und Kunden? Um eine reibungslose Kommunikation zu gewährleisten werden externen Partnern oft Remote-Zugriffe auf diverse Systeme des Unernehmens (webbasierte Anwendungen oder Portale) erlaubt. Da die internen Sicherheitsverantwortlichen wenig bis keine Kontrolle über die Sicherheitseinstellungen dieser Fremdgeräte haben, besteht dabei eine akute Gefährdung der Unternehmung.

Heute wird viel Vertrauen in den Einsatz der VPN-Technologien (Virtual Private Network) gesetzt. Mit VPN wird die Vertraulichkeit der Daten gewährleistet, da das Mitlesen im Internet verhindert wird. Auf dem Markt gibt es viele – auch preiswerte – VPN-Lösungen. So können Mitarbeiter, Partner und Kunden verschlüsselt auf das Firmennetz zugreifen. Einsatz der VPN-Technologien ohne zusätzliche Massnahmen genügt indes den heutigen Sicherheitsansprüchen nicht mehr. Ein ungesichertes Endgerät kann trotz VPN-Technologie das Firmennetz und vertrauliche Daten gefährden.

> Einsatz der VPN-Technologien ohne zusätzliche Massnahmen genügt den heutigen Sicherheitsansprüchen nicht mehr.

Die primären Gefährdungen stellen Viren, Würmer, Trojaner, Spyware und andere Malware-Typen dar. Ein verseuchtes Endgerät kann das Firmennetz – eventuell sogar durch eine VPN-Verbindung – infizieren. Viren, welche früher Tage oder Wochen brauchten, um sich auszubreiten, verbreiten sich heute innert wenigen Minuten im Internet. Durch ihren steigenden Einsatz werden PDA wohl immer häufiger das Ziel von Angriffen sein. Die Gefahr von PDA-orientierter Malware ist aber noch nicht allen bekannt.

In erster Linie müssen die Unternehmen das Problem erkennen und entsprechende Sicherheitsrichtlinien für den Einsatz von Endgeräten definieren («End Point Security Policy»). Anschliessend muss sichergestellt werden, dass nur noch Geräte auf das Firmennetz zugreifen können, welche diese Sicherheitsrichtlinien erfüllen. Als Sicherheitskriterien können beispielsweise folgende Parameter geprüft werden:

- Betriebssysteme inklusive Versionen,
- Aktuelle Patches,
- Sicherheitseinstellung auf dem System,
- Anti-Virus-Schutz (Typ, Version usw.),
- Einsatz einer persönlichen Firewall und deren Einstellungen,
- VPN-Einstellungen,
- Installierte Software.

Die Tauglichkeit der Lösung steht und fällt damit, dass es sowohl für Hacker als auch für Mitarbeiter unmöglich ist, sie zu manipulieren oder zu deaktivieren. Wirkungsvolle Sicherheitsrichtlinien für den Einsatz von Endgeräten müssen durchsetzbar sein. Dazu müssen entsprechende Kontrollmechanismen die Einhaltung der «End Point Security Policy» sicherstellen. Im Hinblick auf die Vielfalt von Endgeräten ist dies keine leichte Aufgabe. Doch es lohnt sich, sich dieser Herausforderung zu stellen. ■

Der Autor
Ivan Roman, Trainer und Consultant bei Roman Consulting & Engineering AG, Zürich.
www.roman.ch

Unsere Experten beantworten Ihre Fragen. Schreiben Sie uns: it-security@computerworld.ch

Ein Archiv der Helpdeskartikel finden Sie im Internet: www.computerworld.ch