So werden mobile und Heimarbeitsplätze sicherer

Der mobile Arbeitsplatz – ein Sicherheitsrisiko

Das unkomplizierte Arbeiten von zuhause wird immer beliebter. Kleinere wie auch grössere Firmen nutzen die Möglichkeit, ihre Mitarbeiter von zuhause oder von unterwegs auf ihre Systeme zugreifen und Arbeiten erledigen zu lassen. Die Verbindung geschieht dabei oft mittels VPN, da es schnell umgesetzt und kostengünstig ist. Doch der schnelle Zugang birgt einige Gefahren, die es nicht zu unterschätzen gilt.

Andreas Wisler ist Geschäftsführer der GO OUT Production GmbH mit Sitz in Wiesendangen, welche sich mit IT-Sicherheitsüberprüfungen und -beratungen auseinandersetzt. Weitere Informationen sind unter www.goSecurity.ch abrufbar, 052 320 91 20, wisler@goout.ch

«Diese Arbeit kann ich gut am Samstag von zuhause aus erledigen», hört man immer öfters. Viele Firmen gestatten es ihren Mitarbeitern, mit dem Laptop oder dem eigenen Heimarbeitsplatz von extern auf die Systeme zu gelangen und Arbeiten zu erledigen. Der Vorteil für die Firmen liegt ganz klar in der Flexibilität: arbeiten zu jeder Zeit. Auch kann sich eine Firma so einen zusätzlichen Arbeitsplatz sparen. Für die Administratoren bedeutet es zudem, bei einem Alarm nicht mehr in die Firma rennen zu müssen um festzustellen, dass es nicht dringend ist, sondern sie können ganz bequem vom Sofa aus das Problem eruieren und falls nötig lösen.

Flexibilität birgt Gefahren

Doch oft werden die mit der Flexibilität verbundenen Gefahren vergessen. Am 7. Oktober 2003 bewies die Schweizerische Post, wie schnell sich diese Gefahr zum Worst-Case-Szenario ausdehnen kann. Ein Programmierer hatte unabsichtlich bei einer Aktualisierung den Wurm SQL Slammer in die Produktion eingeschleppt. Kurze Zeit später musste die Post ihre Datenbank-Server vom Netz trennen. Die Folge davon: Ein- und Auszahlungen am Schalter, Bezüge am Postomat oder das Yellownet funktionierten nicht mehr.

Vielen Firmen ist nicht bewusst, dass bei den meisten Firewall-Typen eine VPN-Verbindung wie ein interner Benutzer betrachtet wird. Der Verkehr wird weder auf Viren, Würmer noch auf andere schädliche Software hin untersucht.

Trojaner auf dem Heimarbeitsplatz nutzen vermehrt diesen Punkt aus und versuchen, Informationen durch geöffnete VPN-Verbindungen zu ergattern und an die Konkurrenz weiterzuschicken. Der Schädling sitzt unbemerkt auf dem Rechner des Heimbenutzers und wartet, bis eine Verbindung aufgebaut wird. Vor zirka einem halben Jahr flog in der Schweiz ein solcher Betrug auf. Ein Mitbewerber stahl unbemerkt die Interesse- und Offertanfragen und leitete diese auf den eigenen Computer um. Das Gerichtsverfahren ist immer noch im Gange.

WLAN öffnet Tür und Tor

Eine weitere Gefahrenwelle besteht, wenn der heimische Rechner mit mehreren Personen geteilt wird. Vor allem Kinder decken ihre Neugierde nach Spielen, Chatten und Informationen im Internet. Schon länger sind Schwachstellen zum Beispiel im Internet Explorer bekannt, mit welchen beim Besuch einer manipulierten Internetseite unbemerkt schädliche Software installiert werden kann. Dies kann fatale Folgen haben, wenn sich ein solchermassen verseuchter Rechner anschliessend mit der Firma verbindet.

Aus diesem Grund stellen einige Firmen ihren Mitarbeitern einen Laptop zur Verfügung, welcher nicht mit anderen Personen geteilt werden darf. Mit der Installation des Antivirenprogramms und den aktuellen Patches durch die IT sind die Schutzmassnahmen aber oft beschränkt. Auch hier lauern Gefahren. Vor allem Manager nutzen die Möglichkeit, von jedem Ort der Welt ihre E-Mails, Termine und Daten im Büro abzurufen. Sei dies nun vom Hotel aus oder am Flughafen/Bahnhof per Wireless LAN (WLAN) . Gerade Wireless-LAN-Verbindungen öffnen einem potenziellen Angreifer Tür und Tor. Die Verbindung zum öffentlichen Hotspot ist unverschlüsselt und eine Personal Firewall fehlt meistens auf dem mobilen Gerät. Ein Kinderspiel, den fremden Rechner zu «entern».

Drei mögliche Schutzmethoden

Wenn man sich dieser Gefahren bewusst ist, stellt sich automatisch die Frage, wie man sich davor schützen kann. Auch die Hersteller von Sicherheitslösungen haben erkannt, dass Handlungsbedarf besteht, und präsentieren verschiedene Lösungsansätze. So behandeln zum Beispiel Firewalls VPN-Benutzer wie externe Verbindungen, Quarantänefunktionen kontrollieren den Schutzstand des Clients oder Web-Applikationen ermöglichen eine «gefilterte» Ansicht auf Programme und Daten. Diese drei Methoden stellen nur einige Möglichkeiten dar, sich optimal zu schützen, und werden im Folgenden ausführlicher beschrieben.

Firewall mit «VPN-Interface»

Firewalls, die VPN-Verbindungen nicht direkt in das interne Netzwerk verbinden, erlauben es, verschiedenen Richtlinien zur Steuerung der Verbindung zu definieren. So können zum Beispiel nur wenige, explizit bestimmte Dienste durch die Firewall hindurch zugelassen werden. Diverse Marktstudien haben ergeben, dass die meisten Anwender unterwegs vor allem über aktuelle Termine und Aufgaben informiert werden möchten und jederzeit Zugriff auf ihre E-Mails wünschen. So reicht es, wenn nur diese Systeme von aussen erreichbar sind. Zusätzlich kann die Verbindung auf einen Terminal oder Citrix-Server zugelassen werden. Viren können sich über diesen Weg nicht verbreiten, ein Arbeiten in der gewohnten Umgebung und mit den eigenen Daten ist jedoch weiterhin problemlos möglich. Zudem sind der Unterhalt und die Konfiguration für die IT-Administratoren relativ gering.

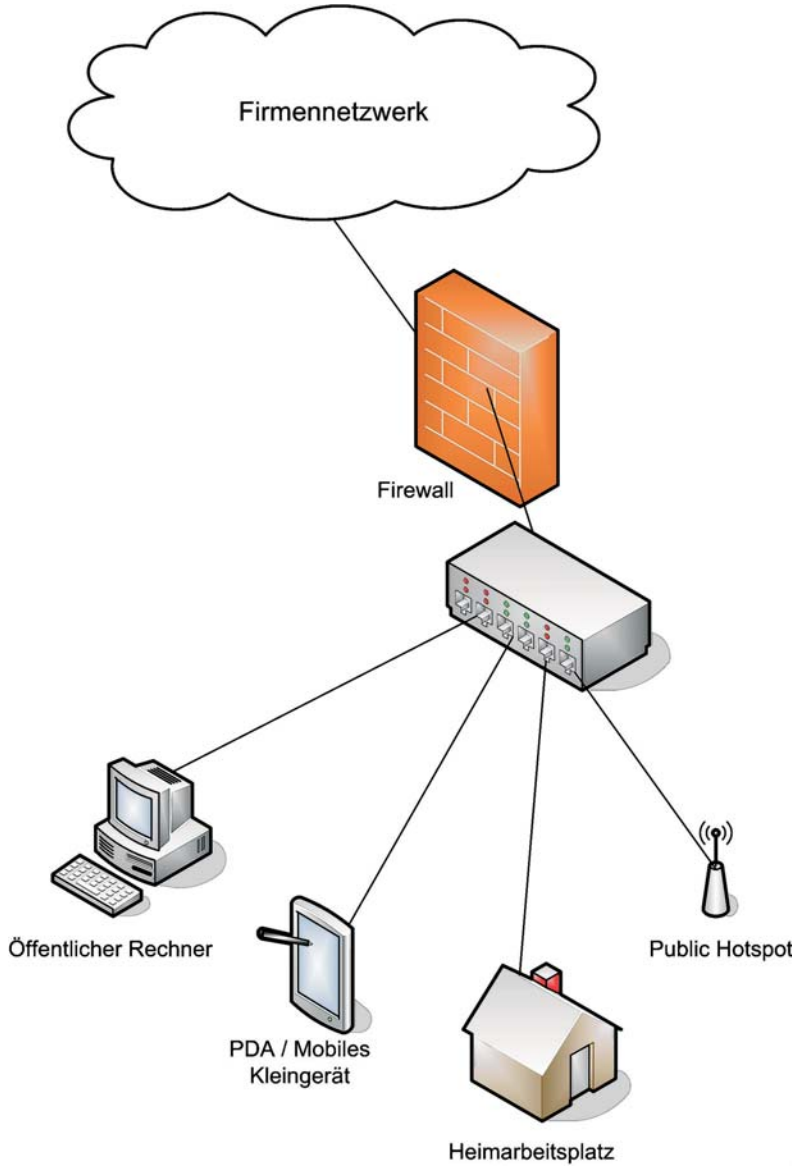
Quarantänefunktion

Der Windows-Server 2003 sowie der ISA-Server 2004 ermöglichen es, einen Benutzer, bevor er via VPN in das Firmennetzwerk gelangt, in eine Quarantäne «einzusperren». In dieser Quarantäne können diverse Skripts auf dem Heimrechner gestartet werden. So kann beispielsweise kontrolliert werden, ob der Virenscanner auf diesem Rechner aktuell ist, ob alle Patches korrekt installiert wurden und ob die Windows-Firewall aktiv ist. Erst wenn diese Tests erfolgreich abgeschlossen wurden, wird die Verbindung in das Firmennetzwerk zugelassen. Microsoft nennt diese Technik «VPN Quarantine Control Feature». Die vorhandenen Schutzmöglichkeiten werden weiterhin ausgebaut. So soll es später auch möglich sein, diese Technik für DHCP, IPsec und Wireless-Funktionen auf Basis 802.1x anzuwenden. Die Roadmap und weitere Informationen hat Microsoft unter http://www.microsoft.com/NAP bereitgestellt.

Web-Applikationen

Eine andere Richtung schlagen die Web-Services ein. Über den gewohnten Browser auf dem Laptop, dem Rechner zuhause oder gar über einen öffentlichen Computer kann eine Verbindung auf einen Server in der Perimeterzone (auch als DMZ bezeichnet) der Firma aufgebaut werden. Alle Anwendungen werden so angepasst, dass sie im Internet-Browser angezeigt und bearbeitet werden können. Der Server wiederum holt die Daten im internen Netzwerk. So besteht keine Gefahr, dass sich ein Virus durch die verschlüsselte Verbindung von aussen via Perimeterzone ins interne Netzwerk einschleichen kann.

Dies sind nur drei Methoden, die die Sicherheit stark erhöhen und leicht in bestehende Umgebungen implementiert werden können. Alle Massnahmen zeigen jedoch nur Wirkung, wenn eine Sicherheitsrichtlinie den Umgang mit Verbindungsdaten, Informationen zum Netzwerkaufbau, der Geheimhaltung von Benutzername und Passwort klar regelt. Die Technik stellt nur Möglichkeiten zur Wahrung und zum Aufrechterhalten der Sicherheit dar. Der Mensch hinter dem Rechner trägt seinen Teil zur sicheren Kommunikation bei. Technik und Sensibilisierung helfen, dass sich keine schadhafte Software im internen Netzwerk verbreiten kann.



Viele verschiedene Wege ermöglichen einen Zugriff auf das Firmennetzwerk. Sei es von einem öffentlichen Rechner aus, per PDA, von zuhause oder per Wireless LAN – alles neue Gefahrenpotenziale, die es zu kontrollieren gilt