

Hintergrundartikel

Effiziente Endpoint Security am Arbeitsplatz

Oftmals betrachten Unternehmen die eigene Belegschaft als eines der größten Risiken für die IT-Sicherheit. Dabei muss man differenzieren: Nur ein kleiner Teil der Mitarbeiter verfügt über kriminelle Absichten und die Energie, diese in die Tat umzusetzen. Wesentlich häufiger veranlassen unmittelbare persönliche Interessen zur Umgehung von Sicherheitsschranken. Dazu gehört zum Beispiel der Wunsch, eine bestimmte private Anwendung zu nutzen oder Prozesse vermeintlich „abzukürzen“. Sicherheitsschranken werden hier nur als lästig und überflüssig empfunden, sodass sich auch das Unrechtsbewusstsein in Grenzen hält. In Verbindung mit einem nach wie vor relativ sorglosen und unwissenden Umgang mit Gefahrenquellen entsteht so eine brisante Mischung, die Unternehmen nicht ignorieren können.

Die zur Verfügung stehenden Möglichkeiten für Mitarbeiter, etablierte Sicherheitsmaßnahmen zu umgehen, nehmen zu: So erfreuen sich Instant Messaging- und Internet Telefonie-Programme (z.B. ICQ, AIM oder Skype) einer ungebrochenen Popularität. Verbreitet ist auch die Nutzung von RSS-Feeds oder Peer-to-Peer-Filesharing auf dem Unternehmens-PC oder Laptop. Dass dadurch höchst gefährliche Dateien und Malware eingeschleust werden können, wird von den Mitarbeitern gerne ignoriert. Im Falle von Filesharing kommen auf das Unternehmen unter Umständen sogar rechtliche Konsequenzen zu, wenn illegale Dateien getauscht wurden.

Ein weiteres drängendes Problem ist die an sich erfreuliche Verbreitung von kostengünstigen WLAN- und UMTS-Zugängen samt entsprechendem

Equipment. Für die schnelle Konnektivität sind Mitarbeiter gerade auf Dienstreisen gerne bereit, die installierten Firewalls, Anti-Viren-Scanner, URL-Filter & Co. außer Kraft zu setzen – und damit das System für beliebige Angriffe zu öffnen. Ebenso verhält es sich bei der Verbindung von geschäftlichen mit privat genutzten Systemen via Bluetooth, FireWire oder USB.

Wirklicher Schutz kann angesichts dieser Situation nur durch den Einsatz von Endpoint-Security-Clients erreicht werden, die den Zustand des Arbeitsplatzes laufend überprüfen und Policy-Vorgaben des Unternehmens umsetzen. So kann zum Beispiel die Deaktivierung von drahtloser Kommunikation am Arbeitsplatz verhindert und bei Bedarf für Dienstreisen wieder flexibel erlaubt werden. Ziel der IT-Sicherheit muss zudem ein übergreifendes Network Access Control (NAC)-System sein, das nur Policy-konformen Clients die volle Teilnahme am Unternehmensnetz ermöglicht. Probleme wie die oben erwähnten Peer-to-Peer- und Instant Messaging-Programme lassen sich über entsprechende Gateway-Security-Erweiterungen an zentralen Verkehrsübergangspunkten im Netz des Arbeitgebers gut filtern und je nach Policy selectiv erlauben oder blocken. RSS-Feeds sollten zentral am Gateway nach Viren gescannt werden - wiederum wird dies am Gateway zentral erledigt. Aus der Perspektive der IT-Sicherheit wird der Mensch immer ein „Sicherheitsrisiko“ bleiben. Trotzdem lassen sich negative Auswirkungen heute durch technische Lösungen auf ein absolutes Minimum begrenzen.

Über phion:

Die phion AG ist einer der führenden europäischen Anbieter für Lösungen zum Schutz der Unternehmenskommunikation. Mit dem netfence-Produktportfolio bietet phion Lösungen für höchste Ansprüche an Verfügbarkeit, Sicherheit und Management. netfence-Appliances adressieren konsequent sämtliche sicherheitsrelevanten Aspekte: Von der Verteidigung am Perimeter über die sichere und hochverfügbare Anbindung von Filialen bis hin zur Abwehr gefährlicher Inhalte und dem Schutz des internen Netzwerks. Webapplikationen wie e-Banking-Plattformen und Web Services werden von ‚airlock‘ vor Angriffen und Missbrauch geschützt. Alle phion-Produkte verfügen zudem über ein zentrales Management und zeichnen sich durch besonders günstige TCO aus. phion ist im mid market Segment der Wiener Börse gelistet (Kürzel: PHIO) und hat Hauptsitze in Innsbruck, Österreich sowie Zürich, Schweiz. Zu den Kunden von phion zählen namhafte, international tätige Unternehmen aus allen Branchen.