Vernetzung birgt Gefahren
IT-Sicherheit für Architekten- und Ingenieurbüros

Lutz Hausmann, Lüneburg

Umfassende IT-, Dokumenten- und Kommunikationssicherheit

Bei diesen Erfordernissen kommt man nicht umhin, sich mit Sicherheitssystemen zu befassen. Die Konfrontation mit einer Unmenge von Security-Systemen, einer Vielzahl von undurchschaubaren Bedrohungen wie auch gesetzlichen Maßgaben ist dabei die Folge. Zwar gehören heute in der Regel Firewall und Anti-Virus-Programme zum Standard eines jeden Büros, aber die Bedrohungen haben sich gewandelt und daher werden völlig neue Funktionen zusätzlich benötigt. Die Folge: ohne umfassende Konzepte greift die Abwehr oftmals ins Leere.

IT-Verantwortliche wissen heute, wie fatal sich diese Risiken auswirken können. Dagegen steht, dass die meisten Ingenieur- und Architekturbüros begrenzte finanzielle und personelle Ressourcen haben. Gleichzeitig sind jedoch die Anforderungen auch durch den Gesetzgeber gestiegen. Wer heute von Sicherheit spricht, meint umfassende Sicherheit für die IT, sowohl für elektronische Dokumente als auch für die Kommunikation. Für größere Organisationen ist dies naturgemäß einfacher zu erreichen als für kleine Büros oder sogar einzelne Architekten und Ingenieure. Dort fehlen oft Ressourcen und Expertise, um aus den verfügbaren Lösungen ein schlüssiges Gesamtkonzept zu entwickeln.

Standards, die erfüllt werden müssen, aber nicht ausreichen

Firewall, Virenschutz und Spam-Abwehr sind heutzutage zentrale Sicherheitsfunktionen, die in fast jedem Architektur- und Ingenieurbüro zu finden sind. Firewall-Regeln erlauben es, die Kommunikation grundsätzlich zu reglementieren. Dazu gehört auch, Maßnahmen zeitabhängig zu definieren und ganz wichtig: zu protokollieren.

Ob ein eigener Mailserver in der Organisation vorhanden ist oder ein Email-Dienst wie GMX oder Yahoo verwendet wird, das Viren-Scanning muss in jedem Fall automatisch im Hintergrund erfolgen. Genauso muss beim Surfen jede Seite im Internet nach Viren on-the-fly untersucht werden. Spam-Mails sind für die meisten nur lästige Nebeneffekte, doch sehr oft nutzen Angreifer Spam-Mails, um Trojaner einzuschleusen. Diese Programme werden für jedes Zielobjekt neu programmiert, so dass Virenscanner oft an ihren Attacken scheitern, da sie schneller sind als ein Virenpattern-Update auf dem Markt ist. Ein gut eingestellter Spam-Filter hingegen lässt die Mail gar nicht erst bis zum Arbeitsplatz durch.

Ein Schritt weiter: Webseiten-Kontrolle

Wenn man seinen Mitarbeitern Zugriff auf beliebige Portale erlaubt, ist das sowohl eine Frage der Arbeitskosten als auch der Systemsicherheit. Ein detailliert einstellbarer Content-Filter erleichtert die Kontrolle über die betrachteten Webseiten enorm. Unbemerkt für den Anwender blockt ein Filter Webseiten nach unterschiedlichen Kategorien, wie Pornographie, Auktionen, Shopping und vieles mehr. Denn Gefahr droht Arbeitsplätzen nicht nur durch aktive Angriffe. Immer wieder werden Sicherheitslücken in Web-Applikationen gefunden, die nur durch Anzeigen einer Webseite aktiv werden. Meist werden dann Spyware und im schlimmsten Fall Keylogger und Backdoor-Programme von diesen Seiten auf den eigenen Computer geladen. All-in-One Geräte (so genannte UMT Appliances) blocken solche Angriffe, in dem sie nicht korrekte Pakete im Datenstrom finden und aussperren oder eine Webseite von vorn herein nicht durchlassen.

Verschlüsselte Kommunikation, ein MUSS

Vertrauliche Korrespondenz zwischen Ingenieur, Architekt und Auftraggeber kann ohne Risiko des Ausspionierens oder der Veränderung über das Internet mittels einer UTM.Appliance (Universal Thread Management) versendet werden. Auch eine zeitliche begrenzte Anbindung von Mitarbeiter, Partner oder Auftraggeber an das Netzwerk des Büros ist ohne weiteres und sicher umsetzbar. Vom Hotel

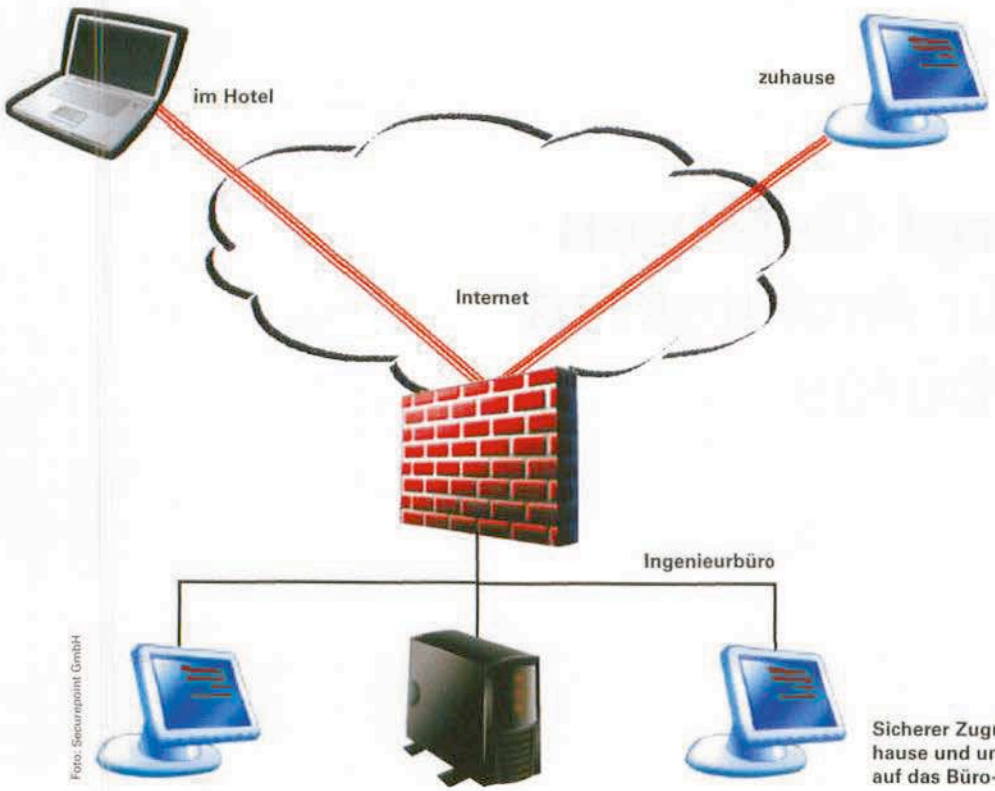

Foto: Securepoint GmbH

Sicherer Zugriff von Zuhause und unterwegs auf das Büro-Netzwerk

aus oder von Zuhause mit dem Laptop kann ebenfalls über jede beliebige Internetverbindung ein sicherer Zugang zum Büro erfolgen.

Die EV-basierte Kommunikation mit Mitarbeitern, Partnern, Korrespondenzbüros oder Niederlassungen kann hierbei uneingeschränkt über das Internet unter Ausnutzung aller üblichen Programme in verschlüsselter Form und reglementiert durchgeführt werden. Die Größe von Daten ist nicht begrenzt. Auch bei Übertragungsunterbrechung kommt es nicht zum Datenverlust. Man kann mit Auftraggebern und Mitarbeitern auch in Echtzeit per normaler Datenübertragung, IP-Telefonie, Instant Messaging („Chat"), kommunizieren und sogar Videokonferenzen durchführen – allesverschlüsselt! Dadurch spart man viel Zeit und Kommunikationskosten in anderen Bereichen ein, ebenso ist die Integrität von Dokumenten gesichert. Das VPN ermöglicht den autorisierten Mitarbeitern und Partnern einen schnellen und absolut sicheren Zugang über das Internet auf Dokumentensammlungen, Datenbanken, Berichtsablagen und vieles mehr.

Zur sicheren Authentisierung wird dabei nicht auf das Einloggen mit Benutzernamen und Passwort vertraut. Schließlich lassen sich solche Zugangsdaten erschleichen oder erraten. Mehr Schutz bietet eine Public-Key Infrastructure (PKI), die verschlüsselte Zertifikate zur Signatur und Kontrolle verwendet. Ein in die Security-Appliance integrierter PKI-Server kann das Management erheblich vereinfachen, vor allem, wenn er in die Sicherheitsstruktur der Appliance eingebunden ist. Auch werden die jeweiligen Einlog-Zeiten der Anwender dokumentiert und können unter anderem zur Zeiterfassung und Kontrolle verwendet werden. Denn neben dem Schutz des Netzwerkes und der Kommunikation ist die Analyse aller Aktivitäten, das Reporting und die direkte Alarmierung ein wichtiger Standard jeder Sicherheitslösung. Sowohl aus rechtlicher als auch aus ökonomischer Sicht ist es wichtig, stets nachweisen zu können: „Wann ist was passiert und wer hat was getan!"

Gesamtlösung in einem System für jede Organisationsgröße

Umfassender Schutz ist das Ziel jedes Sicherheitskonzepts. Doch je mehr Bereiche inbezogen sind und je enger der Abwehrkreis gewählt wird, desto komplexer werden die Security-Policies. Eine flexible und langfristige Lösung bieten dafür Sicherheits-Appliances – so genannte Unified Threat Management (UTM) Systeme – die alle Komponenten für ein wirkungsvolles Schutzkonzept unter einem Dach vereinen. UTM bedeutet, alle wichtigen Sicherheitsbedürfnisse unter guten Anwendungs- und Kostengesichtspunkten in einem System zusammenzufassen. Statt Firewall, Router, VPN-Server, Content-/Spam-Filter und Virenschutz von verschiedenen Herstellern zu beziehen, gehen viele Anwender deshalb einen anderen Weg. Sie sichern das IT-Gesamtsystem mit einem integrierten Produkt ab und müssen so keine unterschiedlichen Teillösungen miteinander kombinieren und können damit unnötige Komplexität und Kosten vermeiden.

Autor

Lutz Hausmann
Lutz Hausmann ist Gesell-schafter und Geschäftsführer der 1997 gegrün-deten Securepoint GmbH in Lüneburg und seit 1994 als Berater und technischer Leiter im Bereich der IT-Security für Unternehmen tätig. Er studierte Informatik an der Universität Hamburg. Die Securepoint GmbH schützt seit ihrer Gründung rund 20000 Unternehmensnetzwerke aus allen Behörden- und Wirtschaftsbereichen.

Informationen: www.securepoint.de