Sieben Sicherheitsprobleme die gerne übersehen werden

Wie wichtig die Sicherheit Ihres Unternehmensnetzwerks ist, das wissen Sie genau. Und Sie wissen auch, was Sie riskieren, wenn Sie gegen eine Bedrohung nichts unternehmen. Vermutlich machen auch Sie sich oft Sorgen über die schlimmen Konsequenzen von Wirtschaftsspionage und mangelnder Datensicherheit – richtig?

Und das aus gutem Grund. Denn wenn vertrauliche Daten in die falschen Hände geraten, kann das verheerende Konsequenzen haben: Wenn Ihr Netzwerk einem Hacker-Angriff nicht standhält, sind Kundendaten und auch Kundenbeziehungen gefährdet. Ihre Aktien und Ihr Markenwert rutschen in den Keller. Das Wohlwollen der Verbraucher ist schnell unwiederbringlich verloren. Die Kosten, die ein Angriff auf ein Unternehmensnetzwerk nach sich zieht, sind nicht bekannt – und möglicherweise auch nicht messbar.

Doch das Schlimme ist: Möglicherweise sind Sie sich nicht sämtlicher Bedrohungen für Ihre Umgebung bewusst. In diesem Whitepaper stellen wir Ihnen deshalb sieben Sicherheitsprobleme vor, die oft übersehen werden. Diese Sicherheitslücken gefährden Ihr Netzwerk, Ihre Unternehmensdaten und – nebenbei bemerkt – auch Ihren Job.

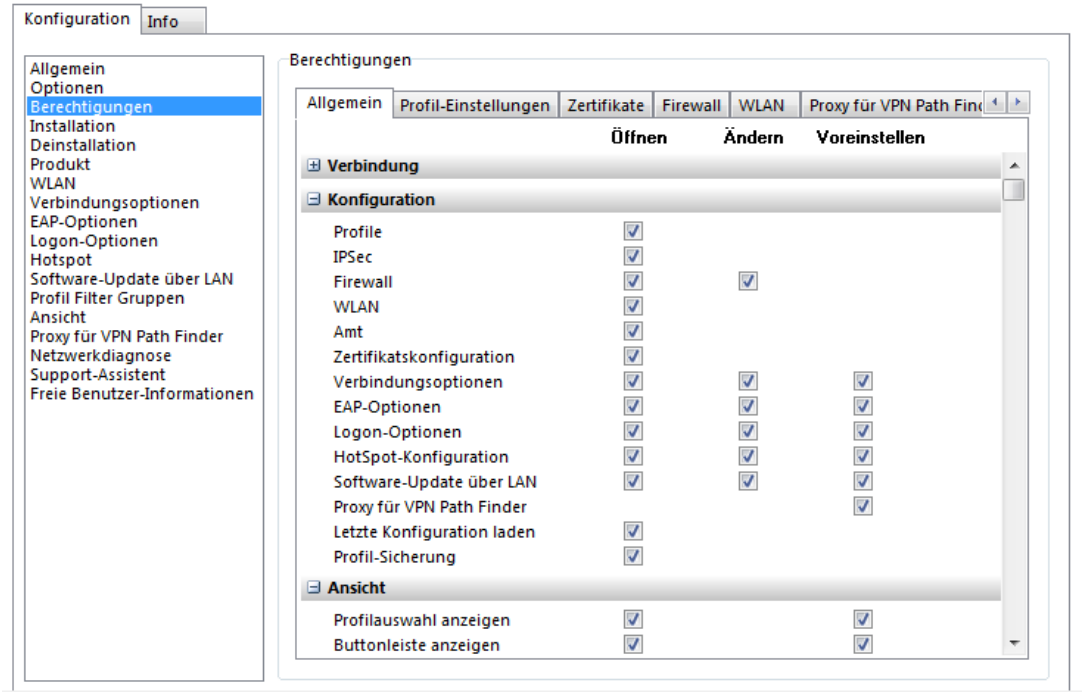
1. Skrupellose Mitarbeiter
2. Private Geräte entziehen sich der Kontrolle
3. Schwachstelle: Sicherheitslösungen von einem Anbieter
4. End-of-Life: EOL-Software ohne Sicherheits-Updates
5. Sicherheitslösung schließt neue Technologien aus
6. Sicherheitslösungen und Richtlinien passen nicht zueinander
7. Schatten-IT: Abteilungen beschaffen sich eigene IT-Ressourcen
8. Seien Sie ein Held!

1. Skrupellose Mitarbeiter

Wenn Mitarbeiter selbst die Initiative ergreifen, um die Sicherheitseinstellungen ihren eigenen Produktivitätsanforderungen anzupassen, setzen sie möglicherweise wichtige Sicherheitsvorkehrungen außer Kraft. So sehr Sie Ihren Mitarbeitern auch vertrauen: Dass alle das Thema Sicherheit genauso ernst nehmen wie Sie, kann nicht vorausgesetzt werden. Viele Bedrohungen entstehen durch Nutzer, denen

nicht bewusst ist, dass sie vielleicht einem Hacker die Tür öffnen. Entweder, weil sie in puncto Sicherheitstechnologien naiv sind oder weil sie ihre Aufgaben so zügig wie möglich erledigen wollen. Manchmal treffen auch beide Gründe gleichzeitig zu.

Ein Beispiel: Ein Mitarbeiter nimmt einen unternehmenseigenen Laptop mit nach Hause. Weil die Endgeräte-Firewall aktiv ist, kann er an seinem eigenen Drucker keine von dem Laptop ausgehenden Dokumente ausdrucken. Ohne die Absicht, den Laptop oder das Netzwerk zu gefährden, deaktiviert der Nutzer nun möglicherweise die Firewall, damit er drucken kann.



Parametersperren für User

Und noch ein Beispiel: Ihre mobilen Mitarbeiter arbeiten via VPN. Die Geräte sind so konfiguriert, dass nur Internet-Verbindungen via VPN erlaubt sind. Nun möchte ein Mitarbeiter persönliche Angelegenheiten online erledigen – und zwar außerhalb der sicheren Verbindung. Vielleicht möchte er auf Ressourcen in seinem Heimnetzwerk zugreifen oder im Internet surfen. Der Nutzer ändert kurzerhand die Konfiguration des VPN-Clients, sodass der Online-Verkehr frei verfügbar ist.
Den beiden Mitarbeitern möchte natürlich niemand die Nutzung von Tools zur Produktivitätssteigerung

vorwerfen. Doch das unberechenbare Verhalten der Nutzer ist ein großes Risiko für den Firmen-Laptop. Die neue Konfiguration von VPN oder Firewall wird dadurch schwierig. Die Mitarbeiter sind nicht nur für eine kritische Sicherheitsbedrohung verantwortlich. Sie haben darüber hinaus auch wertvolle Zeit und Ressourcen verbraucht, die nun für die Behebung des Problems eingesetzt werden müssen.

Doch wie können Sie Ihre Mitarbeiter davon abhalten, in dieser gefährlichen Form Eigeninitiative zu ergreifen? Kontinuierliche Schulungen könnten helfen, solche Vorfälle zu reduzieren. Grundsätzlich verhindert wird das Problem dadurch allerdings nicht. Sicherer ist eine Software-Lösung mit zentral administrierbaren Firewalls und VPN-Clients. Eine Aktivierung, Deaktivierung oder Änderung durch die Nutzer darf nicht gestattet werden!

2. Private Geräte entziehen sich der Kontrolle

Setzen wir doch mal die Brille der Datensicherheit auf: Was passiert, wenn ein Mitarbeiter Ihr Unternehmen verlässt? Besitzen diese Mitarbeiter etwa private Geräte mit sensiblen Unternehmensdaten? Oder Zugangsdaten für das Netzwerk? Ein gutes Beispiel für ein unzureichendes VPN-Management und mangelhaften Schutz liefert ein Datenverstoß durch einen Ex-Mitarbeiter eines texanischen Energieversorgungsunternehmens. Selbst nachdem seine Tätigkeit für das Unternehmen endete, konnte er das VPN nutzen – und so auf Unternehmensprognosen zur Verbrauchernachfrage zugreifen. Er konnte die Daten manipulieren oder löschen.
Die Vorgehensweise muss an die BYOD-Umgebung angepasst werden. BYOD bezeichnet die Möglichkeit, dass die Mitarbeiter eigene Endgeräte in das Firmennetzwerk integrieren. Dabei ist ein zentrales Management von größter Bedeutung für die Datensicherheit. Die Sicherheitsrichtlinien müssen strengstens eingehalten werden. Um das zu erreichen, verknüpft man am besten den Versorgungsprozess – das User-Provisioning – und das Identitätsmanagement der Mitarbeiter mit der VPN-Verwaltung. Die Verbindung zur Personaldatenbank stellt dann sicher, dass den Geräten ehemaliger Mitarbeiter jeglicher Zugriff auf das Unternehmenssystem verweigert wird, sobald dieser in der Datenbank den Vermerk „Mitarbeit beendet“ erhält.

Außerdem benötigen Sie einen Prozess zur Löschung sämtlicher Unternehmensdaten vom Gerät des Mitarbeiters. Implementieren Sie eine mobile Geräteverwaltung oder Container-Lösung – diese erzeugt eine Arbeitsumgebung auf dem Gerät. So verfügen Sie über eine leicht zu verwaltende Methode zum Löschen sämtlicher Spuren von Unternehmensdaten und Zugriffsinformationen, wenn ein Mitarbeiter das Unternehmen verlässt. Dieses Vorgehen eignet sich auch gut für den Fall, dass ein Gerät verloren geht oder gestohlen wird.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Deutschland · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Amerika: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Telefon: +1 (650) 316-6273 · www.ncp-e.com

Sieben Sicherheitsprobleme die gerne übersehen werden

3. Schwachstelle: Sicherheitslösungen von einem Anbieter

Der Heartbleed-Bug demonstrierte perfekt, wie groß das Risiko ist, wenn man auf nur eine einzige Sicherheitstechnologie setzt. Durch ihn konnten über verschlüsselte Verbindungen Daten ausgelesen werden. Viele Internetdienste, VoIP-Telefone, Netzwerkdrucker und Router waren aufgrund einer zentralen Schwachstelle anfällig für Angriffe. Auch Unternehmen, die sich auf einen Anbieter für sämtliche Sicherheitstechnologien verlassen, bauen vielleicht auf ein trügerisches Gefühl der Sicherheit.

Schauen wir uns ein typisches Szenario an: Ihre Mitarbeiter verbinden sich über viele unterschiedliche Geräte, von verschiedenen Orten aus und mit diversen Verbindungsmedien mit Ihrem Unternehmensnetzwerk. Eine häufige Vorgehensweise beim Schutz des Datenverkehrs ist die Bereitstellung von VPN-Diensten, wobei eine Firewall als VPN-Gateway genutzt wird. Allerdings werden Firewall und VPN von demselben Gerät bereitgestellt. Tritt bei diesem Gerät ein Sicherheitsproblem auf, sind daher beide Dienste betroffen. Nutzen Sie jedoch für VPN und Firewall unterschiedliche Anbieter, wird automatisch eine zusätzliche Schutzschicht aufgebaut. Das liegt daran, dass der Fernzugriff auf das Unternehmensnetzwerk durch zwei Abwehrsysteme anstatt durch eines autorisiert werden muss.

Falls es überhaupt etwas gibt, das dieser Heartbleed-Albtraum uns lehrt, dann dies: Keine einzige Technologie garantiert einen umfassenden Schutz von sensiblen Daten, Unternehmensnetzwerken und privater Kommunikation. Eine vielschichtige Verteidigungsstrategie – welche die hochwertigsten Netzwerk- und Sicherheitskomponenten von verschiedenen Anbietern kombiniert – kann jedoch erheblich zur Abwehr einer Reihe der häufigsten Ursachen für Datenverstöße beitragen.

4. End-of-Life: EOL-Software ohne Sicherheits-Updates

„Never touch a running system!“ oder: „Ändere kein System, solange es funktioniert!“ – das ist oft ein guter Rat, wenn es um Stabilität und gleichbleibende Leistung geht. Geht es allerdings um Sicherheit, könnte diese Denkweise gefährlich falsch sein: Wird ein EOL-Produkt vom Anbieter nicht mehr unterstützt und aktualisiert, werden eventuell auftretende Schwachstellen nicht mehr behoben.

Betrachten wir beispielsweise Windows XP. Dieses Betriebssystem wird nicht mehr unterstützt. Das Risiko, dass ein Angreifer eine vom Software-Hersteller bislang unbemerkte Sicherheits-Lücke entdeckt, ist nicht zu unterschätzen. Wenn Hacker solche Lücken finden, können sie diese Schlupflöcher für ihre Zwecke nutzen! Es gibt solche Bedrohungen auch bei Anwendungen und anderen Tools — nicht nur bei

Betriebssystemen. Doch wie wappnen Sie sich gegen das Risiko eines Angriffs auf ein EOL-Produkt? Und wie reagieren Sie angemessen auf einen Angriff?

Behalten Sie die Übersicht über sämtliche Betriebssysteme und Software-Produkte, die Ihre Mitarbeiter verwenden — und halten Sie die Programme aktuell. Zugegeben, die Migration eines Betriebssystems bedeutet eine Menge Arbeit. Das Gleiche gilt, wenn man feststellt, dass eine über Jahre gewachsene Unternehmenssoftware auf einem neueren Betriebssystem nicht läuft. Dennoch ist ein aufmerksames und systematisches Vorgehen die einzige Möglichkeit, mit vertrauenswürdigen Software-Updates für ein hohes Maß an Sicherheit zu sorgen.

5. Sicherheitslösung schließt neue Technologien aus

Ihre Computerumgebung muss sich mit aktuellen Trends, Tools und Betriebssystemen weiterentwickeln. Doch was geschieht, wenn ältere Sicherheitslösungen und neue IT-Technologien nicht kompatibel sind? Was, wenn Ihre Maßnahmen gegen die aktuellen Sicherheitsbedrohungen nichts bewirken?

Implementieren Sie deshalb rechtzeitig eine ausgeklügelte, anpassungsfähige Sicherheitslösung und kombinieren Sie die Dienste verschiedener Anbieter. Neue Technologien, zum Beispiel IF-MAP, ermöglichen die Kommunikation und Interaktion zwischen den Lösungen verschiedener Anbieter. So kann auf Bedrohungen schneller und flexibler reagiert werden.

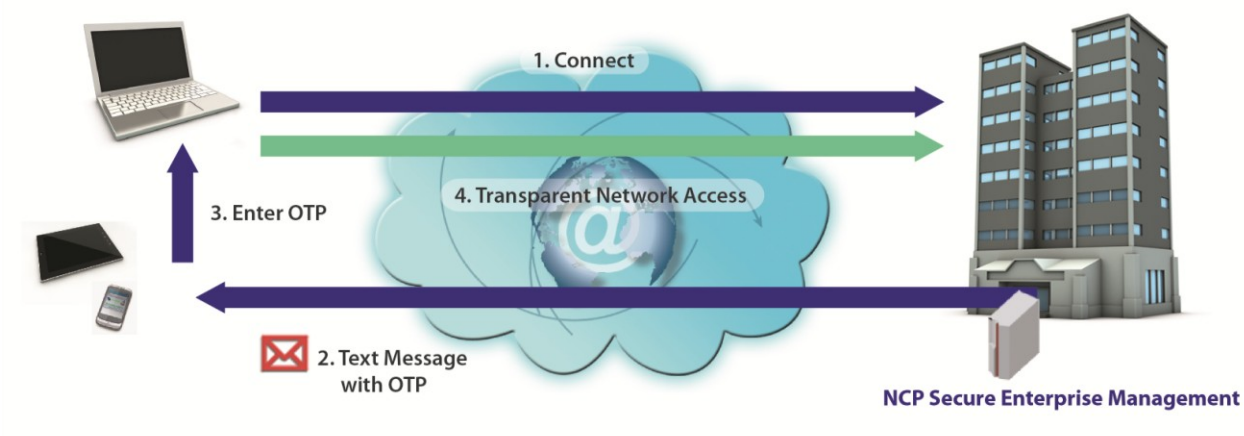
6. Sicherheitslösungen und Richtlinien passen nicht zueinander

Im Zusammenhang mit der Anpassungsfähigkeit Ihrer IT und Ihres Netzwerks gibt es ein weiteres Problem. Was geschieht, wenn Ihre Sicherheitslösungen nicht kompatibel mit den für Ihr Unternehmen geltenden Sicherheitsrichtlinien sind? Was tun, wenn Ihre Lösung die für die Sicherheit erforderlichen Features und Funktionen nicht zur Verfügung stellt? Entscheiden Sie sich für eine flexible Lösung, mit der Sie die Struktur Ihrer Sicherheitsrichtlinien, -verfahren und -systeme unterstützen können.

Einige Sicherheitsanbieter bieten eine Benutzerauthentifizierung lediglich durch Username und Passwort. Die Nutzung von Zertifikaten – PKI – oder einer Zwei-Faktor-Authentifizierung – etwa OTP oder Smartcards – wird dagegen nicht unterstützt. Verlangen Ihre Unternehmensrichtlinien jedoch eine Zwei-Faktor-Authentifizierung, sind Sie und Ihr Unternehmen in einer Sackgasse gelandet.

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Deutschland · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Amerika: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Telefon: +1 (650) 316-6273 · www.ncp-e.com

Sieben Sicherheitsprobleme die gerne übersehen werden



Advanced Authentication

Oder denken Sie an Ihr Nutzerverzeichnis. Möglicherweise verlassen Sie sich auf eine LDAP-Lösung wie Active Directory oder Oracle LDAP? Diese liefert ein perfektes digitales Abbild Ihres Unternehmens, das auf Nutzern, Gruppenzugehörigkeit, Rollen und anderen Regeln oder Signalen basiert. Ermöglicht Ihre Sicherheitslösung eine Identifikation der Nutzer nicht nach den Regeln Ihres Nutzerverzeichnisses, könnten Sie gezwungen sein, Ihr Verzeichnis zurückzuentwickeln, damit es den eingeschränkten Funktionalitäten Ihrer Sicherheitslösung entspricht.

7. Schatten-IT: Abteilungen beschaffen sich eigene IT-Ressourcen

Schatten-IT – fast jeder kennt dieses Phänomen, das in den unterschiedlichsten Formen auftritt: Abteilungen beschaffen sich ihre eigenen Server und Speichersysteme, lagern das Management ihrer Datenbank oder ihrer Datenanalyse aus. Wenn die Abteilungen dabei die geschäftlichen Erfordernisse des Unternehmens nicht berücksichtigen oder wenn Sie den Bedarf in den Abteilungen nicht im Einklang mit der Struktur der Gesamtorganisation decken können, ist das Risiko eines gefährlichen Kontrollverlustes erheblich.

Doch wie können Sie die geschäftlichen Erfordernisse berücksichtigen, ohne entscheidende Schutzmaßnahmen zu lockern? Konkrete Regelungen sind entscheidend. Das gilt auch für die Kommunikation zwischen Sicherheitsexperten und Fachabteilungsleitern. Kommunizieren Sie mit den Führungskräften Ihres Unternehmens! Nur dann können Sie sichere IT-Richtlinien einführen. Kennen Sie die geschäftlichen Anforderungen und die Bedürfnisse Ihrer Mitarbeiter nicht, dann können Sie diese Richtlinien nicht durchzusetzen. Wichtig ist, dass Sie Diskrepanzen zwischen Sicherheitsansatz und Unternehmensbedürfnissen überbrücken. So können Sie eine Schatten-IT verhindern.

Sieben Sicherheitsprobleme die gerne übersehen werden

8. Seien Sie ein Held!

IT-Sicherheitsexperten sind moderne Gladiatoren. Ihre Aufgabe ist die Verteidigung von Unternehmensdaten und -netzwerken. Und zwar sowohl gegen bekannte als auch gegen unbekannte Gefahren. Sie sind derjenige, der das Unternehmen vor dem großen Risiko bewahrt. Sie erkennen die Bedrohungen und ergreifen Maßnahmen dagegen.

Sie haben Fragen oder möchten einen Termin für eine Produktdemonstration vereinbaren? Dann rufen Sie uns jetzt unter +49 (0)911 99 68 0 an oder schreiben Sie eine E-Mail an vertrieb@ncp-e.com. Wir freuen uns auf das Gespräch mit Ihnen!

NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Deutschland · Telefon +49 911 9968-0 · Fax +49 911 9968-299
Amerika: NCP engineering, Inc. · 444 Castro Street, Suite 711 · Mountain View, CA 94041 · Telefon: +1 (650) 316-6273 · www.ncp-e.com

Sieben Sicherheitsprobleme die gerne übersehen werden

Julian Weinberger

Julian Weinberger, CISSP, ist Director of Systems Engineering bei NCP engineering. Er verfügt über eine zehnjährige Erfahrung in der Netzwerk- und Sicherheitsindustrie sowie über umfangreiches Fachwissen in den Bereichen SSL-VPN, IPsec, PKI und Firewalls. Julian Weinberger lebt in Mountain View, Kalifornien. Er ist verantwortlich für die Entwicklung von IT-Netzwerksicherheitslösungen und Unternehmensstrategien von NCP engineering. Außerdem bietet er Großkunden des Unternehmens technischen Support für ihre Remote Access-Sicherheitslösungen, sowohl vor als auch nach dem Kauf.

NCP engineering

Seit der Firmengründung 1986 liefert NCP engineering innovative Software. Diese ermöglicht Unternehmen, ihren Remote Access neu zu überdenken und Schwierigkeiten im Zusammenhang mit Aufbau, Verwaltung und Instandhaltung eines sicheren Netzwerkzugangs für Mitarbeiter zu beseitigen. Mit Firmensitzen in Nürnberg, Deutschland, und in der San Francisco Bay Area in Nordamerika hat das Unternehmen weltweit über 35.000 Kunden. Dazu zählen Unternehmen aus den Bereichen Gesundheitswesen, Finanzen, Bildung und Regierung sowie viele Fortune-500-Unternehmen. Zur Betreuung der Kunden hat NCP zusätzlich ein Netzwerk aus nationalen sowie regionalen Technologie-, Channel- und OEM-Partnern errichtet.