8COM
CYBER SECURITY

10 GEBOTE FÜR MEHR CYBER SECURITY

FÜR UNTERNEHMEN

1. Etablieren Sie ein IT-Sicherheitsmanagement

Cyberangriffe machen immer wieder Schlagzeilen und sorgen für hohe finanzielle Schäden. Auch rechtliche Folgen und Reputationsverlust drohen den betroffenen Firmen. Sichern Sie sich deshalb sowohl technisch als auch rechtlich gegen Angriffe ab. Eine professionelle Risikobewertung durch Cyber Security Experten sowie eine zuverlässige Rechtsberatung unterstützen Sie dabei, die Sicherheitsvorkehrungen in Ihrem Unternehmen den aktuellen Anforderungen anzupassen.

2. Verwalten Sie die Benutzerrechte

Admin-Konten haben praktisch uneingeschränkten Zugriff auf Computer und Netzwerke. Sie können Software installieren oder Systemeinstellungen ändern. Viele Viren und Trojaner benötigen diese Admin-Rechte, um einen Rechner erfolgreich zu infizieren.

Nicht alle User müssen über weitreichende Berechtigungen verfügen, um ihrer täglichen Arbeit nachzugehen. Erteilen Sie Benutzerrechte entsprechend der Aufgabenbereiche Ihrer Angestellten und verhindern Sie so, dass Cyberkriminellen durch fahrlässiges oder böswilliges Handeln Tür und Tor geöffnet werden.

3. Schützen Sie Ihre Systeme

Unternehmen und Freiberufler mit schützenswerten Daten sollten für die Verbindung zum Internet eine professionelle Firewall verwenden. Sie schränkt unerwünschten Datenverkehr so ein, dass die Sicherheit Ihres Netzwerks erheblich gesteigert wird. Überprüfen Sie die Konfiguration der Firewall regelmäßig. Setzen Sie zudem ein professionelles Antivirensystem ein, das regelmäßig upgedatet wird. So verfügen Sie zumindest über einen Basisschutz.

4. Speichermedien sicher entsorgen

Speichermedien wie USB-Sticks und Festplatten sollten Sie fachgerecht entsorgen. Wenn darauf sensible Daten gespeichert wurden, überlassen Sie dies am besten einem spezialisierten Dienstleister. Denn das einfache Löschen der Daten reicht nicht aus, um Datensicherheit zu gewährleisten. Datenträger müssen mehrfach überschrieben und physisch zerstört werden, um eine Wiederherstellung der Daten unmöglich zu machen.

5. Setzen Sie nur aktuelle Software ein

Software-Aktualisierungen (Updates) schließen gefährliche Sicherheitslücken in Betriebssystemen und Anwendungsprogrammen. Selbst kleinste Programmierfehler können es Kriminellen ermöglichen, wichtige Sicherheitsfunktionen zu umgehen und so u. a. Schadprogramme in Unternehmensnetze zu schleusen. Die meisten Software-Anbieter bemühen sich, Sicherheitslücken umgehend zu schließen und bieten regelmäßig kostenlose Updates für ihre Produkte an.

Stellen Sie sicher, dass in Ihrem Unternehmen ein zuverlässiges Update- und Patch-Management existiert. Mit veralteten Programmen gibt es keine Sicherheit.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt/Weinstraße | www.8com.de | info@8com.de | +49 6321 48446-0

6. Verzichten Sie auf ein WLAN-Netzwerk im Unternehmen

Vom WLAN-Einsatz in Unternehmen ist generell abzuraten. Können Sie nicht auf kabellose Netzwerke verzichten, muss das Drahtlosnetz professionell aufgebaut sein, damit Aspekte wie Verschlüsselung und Benutzerverwaltung zentral gesteuert werden können. Unverschlüsselte oder schwach verschlüsselte Funknetze dürfen nicht Teil Ihres internen Netzes sein.

7. Vorsicht beim Einsatz von Cloud-Lösungen

Cloud-Lösungen sind praktisch und sparen wertvolle Ressourcen. Sollten Sie Daten aber nicht in einer eigenen Cloud, sondern bei einem externen Dienstleister speichern und verarbeiten, muss Ihnen bewusst sein, dass unerwünschte Zugriffe durch Dritte möglich sein können, sei es durch Hackerangriffe oder im Rahmen von strafrechtlichen Ermittlungsverfahren.

8. Gehen Sie vorsichtig mit E-Mails um

Setzen Sie zuverlässige Verfahren zur E-Mail-Verschlüsselung ein, wenn schützenswerte Daten verschickt oder Rechtsgeschäfte per Mail durchgeführt werden. Bedenken Sie, dass Cyberkriminelle E-Mail-Absenderadressen fälschen können. Schulen Sie Ihre Angestellten, sodass diese stets wachsam sind und richtig mit verdächtigen E-Mails, die Anlagen oder Hyperlinks enthalten, umgehen.

9. Nutzen Sie sichere Zahlungsverkehrsverfahren

Für Einzelüberweisungen eignen sich besonders die Verfahren, bei denen ein TAN-Generator zum Einsatz kommt. Sammelüberweisungen sollten ausschließlich über signaturbasierte Verfahren wie EBICS oder FinTS mit Chipkarte durchgeführt werden. Sofern höhere Geldbeträge transferiert werden, sollten Computer, die für den Zahlungsverkehr genutzt werden, abgesichert und isoliert werden. Speichern Sie niemals Signaturen auf Computern oder im Netzwerk.

10. Machen Sie Ihre Angestellten zu Sicherheitsexperten

Schaffen Sie ein nachhaltiges IT-Sicherheitsbewusstsein bei Ihren Angestellten. Das erreichen Sie z. B. mit regelmäßigen Awareness-Maßnahmen oder einer nachhaltigen Awareness-Kampagne.

8com GmbH & Co. KG | Europastraße 32 | 67433 Neustadt/Weinstraße | www.8com.de | info@8com.de | +49 6321 48446-0