

→ 10 GEBOTE FÜR DIE INTERNETSICHERHEIT

1. Gebot: Bewerten Sie Ihre Risiken

Identifizieren Sie Ihre wichtigen und schützenswerten Daten. Konzentrieren Sie die Sicherheitsmaßnahmen dann gezielt auf die kritischen Daten und Systeme. Restrisiken können oftmals durch eine entsprechende Versicherung abgedeckt werden.

2. Gebot: Strukturierte IT

Arbeitsabläufe und -prozesse müssen standardisiert und weitgehend automatisiert werden. Alle Verantwortlichkeiten und Aufgaben müssen schriftlich und verständlich definiert sein. Dazu gehören u. a. entsprechende Sicherheitsrichtlinien, ein Benutzerrechte- und ein Sicherheitskonzept.

3. Gebot: Update-Management

Hacking-Angriffe nutzen Sicherheitslücken in Betriebssystemen oder der Anwendungssoftware von Computern aus. Ohne ein zentral verwaltetes Update-Management kann die Sicherheit in Ihrem Unternehmen nicht gewährleistet werden.

4. Gebot: Vulnerability Management

In jedem Firmennetzwerk finden sich hunderte Sicherheitslücken, die mithilfe spezieller Programme (Schwachstellen-Scanner) automatisiert gesucht, bewertet und gemanagt werden. Zusätzlich sollten regelmäßig Penetrationstests durchgeführt werden, um weitere nicht automatisch erfassbare Schwachstellen zu identifizieren.

5. Gebot: Firewall & Proxy

Setzen Sie immer eine professionelle Firewall ein, die den Datenverkehr vollständig analysieren kann. Die Firewall sollte verschlüsselte Verbindungen aufbrechen und untersuchen können. Ebenso ist ein Proxyserver in Verbindung mit mehreren Antiviren-Lösungen für das Surfen im Internet notwendig. Idealerweise surfen Ihre Mitarbeiter über isolierte Terminalserver.

6. Gebot: VPN

Verwenden Sie für den Remote-Zugriff auf Ihr Firmennetzwerk eine professionelle VPN-Lösung. Die Authentifizierung sollte zuerst auf Geräte- und dann auf Benutzerebene erfolgen.

7. Gebot: Antiviren-Konzept

Verwenden Sie professionelle Antiviren-Software. Prüfen Sie ausgewählte PCs regelmäßig mit einer Antiviren-Boot-CD. Auf der Firewall oder dem Gateway sollten zudem mehrere Antiviren-Engines eingesetzt werden.

8. Gebot: Mobiles Arbeiten

Alle mobilen Endgeräte und Datenspeicher sollten verschlüsselt und abgesichert werden. Beim Arbeiten außer Haus sollten Sichtschutzfolien zum Einsatz kommen.

9. Gebot: IT-Security Awareness & Schulung

Schaffen Sie ein nachhaltiges IT-Sicherheitsbewusstsein bei Ihren Mitarbeitern. Schulen Sie speziell Ihre IT-Abteilung regelmäßig und fachgerecht.

10. Gebot: Wireless LAN | WLAN

Vom WLAN-Einsatz in Unternehmen ist generell abzuraten. Kann nicht auf ein WLAN verzichtet werden, wird eine professionelle EAPOL-Lösung zur Authentifizierung benötigt.



Erwin Markowsky



www.8com.de



blog.8com.eu



www.tatort-www.de

→ ANTWORTFORMULAR

Telefax +49 (0) 6321 48 446 - 29

☐ Herr

☐ Frau

Vorname, Nachname, Firma

☐ Senden Sie mir bitte weitere Informationen zu der/den folgenden Leistung/en:

- ☐ Praktische Sicherheitsprüfung für Firewall und VPN-Systeme
- ☐ Praktische Sicherheitsprüfung für Webseiten/-shops
- ☐ Praktische Sicherheitsprüfung für den Fall eines Trojaner-Angriffs o. Ä.
- ☐ Vorträge rund um Themen der Informationssicherheit (inkl. Live-Hacking)
- ☐ Vorträge und Maßnahmen für die gezielte Mitarbeitersensibilisierung

E-Mail-Adresse

☐ Außerdem interessiere ich mich für die folgenden Themen:

☐ Kontaktieren Sie mich bitte telefonisch:

Telefonnummer / am besten zu erreichen: Datum, Uhrzeit



Ihr Ansprechpartner:

Lothar Lammer

E-Mail: vortrag-kmn@8com.de

Telefon: +49 6321 / 48 446 - 2521