

Sammlung Checklisten Pocketseminar: Erfülle ich die wichtigsten IT-Sicherheitsrichtlinien?

	ja	nein	unbekannt
Security für den Einzelplatz-PC			
• Ist auf Ihrem System eine Personal Firewall installiert?	C	C	C
• Ist die Personal Firewall auf dem System aktuell, bzw. wird sie regelmäßig aktualisiert?	C	C	C
• Sind alle vom Hersteller Ihres Betriebssystems empfohlenen Sicherheitsupdates installiert?	C	C	C
• Ist Ihr Browser aktuell und mit allen Sicherheitsupdates versorgt?	C	C	C
• Ist Ihr Browser sicher konfiguriert?	C	C	C
• Ist ein lokaler Virenschanner auf dem System installiert und wird dieser permanent aktualisiert?	C	C	C
• Benutzen Sie zum Versand vertraulicher E-Mails eine Verschlüsselungssoftware?	C	C	C
• Sind vertrauliche Daten auf Ihrer Festplatte chiffriert?	C	C	C
• Ist der Zugang zu Ihrem System mit einem Passwortschutz versehen?	C	C	C
• Verwenden Sie sichere Passworte?	C	C	C
• Haben Sie Ihren E-Mail Client sicher konfiguriert?	C	C	C
Security für das lokale Netz			
• Ist Ihr lokales Netz durch eine zentrale Firewall vor dem Internet geschützt?	C	C	C
• Sind die Administratoren der zentralen Firewall für das Produkt ausreichend geschult?	C	C	C
• Wird die zentrale Firewall überwacht und regelmäßig aktualisiert?	C	C	C
• Ist auf der Firewall nur die Kommunikation erlaubt, die tatsächlich benötigt wird?	C	C	C
• Sind vom Internet aus erreichbare Systeme in einem separaten Netzwerksegment (DMZ) aufgestellt?	C	C	C
• Werden ein- und ausgehende Mails sowie lokal versendete Mails zentral auf Viren und andere Schädlinge untersucht?	C	C	C
• Werden die Virensignaturen auf dem zentralen Virenschanner automatisch und regelmäßig (1x pro Tag, mindestens aber im kleinsten Intervall das der Hersteller anbietet) aktualisiert?	C	C	C
• Wird auf den Arbeitsplätzen ein anderes Virenschanner-Produkt eingesetzt als am zentralen Übergang in das Internet?	C	C	C
• Werden Ihre Internet-Downloads zentral auf Schädlinge überprüft?	C	C	C
• Können Sie den Zugang zu dienstlich nicht relevanten Internetangeboten für Mitarbeiter und Auszubildende unterbinden, wenn dies gewünscht ist?	C	C	C
• Verhindert Ihr Mail-Server den Versand und Eingang von SPAM?	C	C	C

Weiterführende Informationen finden Sie im Pocketseminar IT-Sicherheit in den entsprechenden Kapiteln.



Security für drahtlose Netze

- Wird die Administration Ihrer WLAN-Systeme über die Funkschnittstelle unterbunden?
- Verwendet Ihr WLAN eine starke Verschlüsselung (z.B. WPA)?
- Lehnt Ihr Access-Point unverschlüsselte Verbindungen ab?
- Ist der MAC-Filter aktiviert, bzw. erfolgt eine Prüfung der zugelassenen Notebooks via Positivliste?
- Werden zur Verschlüsselung sichere Passworte verwendet?
- Ist die automatische Vergabe von IP-Adressen deaktiviert (wenn möglich)?
- Sind die Access Points in einem separaten Netzwerksegment aufgestellt und von der Firewall geschützt?

Security für Aussendienst und Heimarbeiter

- Wird auf Notebooks und Heimarbeitsplätzen eine Personal Firewall eingesetzt, die zentral administrierbar ist?
- Erfolgt die Kommunikation zu Ihren Standorten und Ihrer Zentrale mit VPN-Techniken verschlüsselt und authentisch (d.h. kein Dritter kann die Daten mitlesen oder unbemerkt modifizieren)?
- Setzen Sie zur Identifikation Ihrer (Remote)Mitarbeiter eine Zwei-Faktor-Authentifizierung ein?
- Sind Heimarbeitsplätze und Notebooks vor Dialern geschützt (nur bei Modem und ISDN)?
- Ist der USB-Anschluß deaktiviert, bzw. ist er durch einen Administrator kontrollierbar?
- Sind die Daten auf Ihren mobilen Systemen verschlüsselt?
- Widmen Sie PDAs und Smartphones bezüglich Ihrer Sicherheit die gleiche Aufmerksamkeit wie Notebooks?
- Sind die Bluetooth- und Infrarotschnittstellen Ihrer Handys, PDAs und Notebooks deaktiviert, wenn Sie diese nicht verwenden?

Security für Betriebssysteme im Allgemeinen

- Sind alle vom jeweiligen Hersteller Ihrer Betriebssysteme und Anwendungen empfohlenen Sicherheitsupdates installiert?
- Verwenden Sie zur Verteilung solcher Updates eine zentrale Lösung?
- Haben Sie einen Informationsdienst abonniert, der Sie über Sicherheitsupdates informiert?
- Wird die interne Umsetzung der aus dem Informationsdienst bezogenen Empfehlungen kontrolliert und sichergestellt?
- Werden Patches und Updates vor der Installation auf einem Referenzsystem getestet?
- Wurden Ihre Anwendungen auf Sicherheitslücken hin überprüft?
- Sollten Sie bei einer Anwendung Sicherheitslücken aufgedeckt haben - Wurden diese beseitigt oder wird die Applikation von einer Spezial-Firewall geschützt.
- Ist der Webserver in einem eigenen Segment aufgestellt und von der zentralen Firewall geschützt?
- Wird Ihr Webserver regelmäßig aktualisiert?
- Falls Sie Webbasierte Anwendungen anbieten - Wurden diese auf Schwachstellen hin überprüft?
- Bieten Sie Ihren Besuchern bei der Übermittlung von Daten einen verschlüsselten Zugang an (SSL)?

Weiterführende Informationen finden Sie im Pocketseminar IT-Sicherheit in den entsprechenden Kapiteln.