Checkliste System-Sicherheit für PC, Notebook und mobile Geräte

Für den sicheren Betrieb von PCs, Notebooks und insbesondere mobilen Geräten wie Smartphones und Tablets sollten Sie die nachfolgenden Punkte beachten. Überprüfen Sie Ihre Installation, ob Sie die aufgelisteten Anforderungen erfüllen. Diese Checkliste liefert Ihnen wichtige Hinweise, kann jedoch keine umfassende Analyse und Beratung ersetzen.

Grundanforderungen:

1) Ist das System mit einem BIOS Password beim Einschalten geschützt? Existiert, wenn möglich, ein separates Password für die BIOS Administration?

2) Ist die Betriebssystem-Anmeldung mit einem Password geschützt? Werden ausschließlich starke Passwörter verwendet (bestehend aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen), die nicht anderweitig auch benutzt werden?

3) Existieren verschiedene Benutzerrollen auf dem System (für Administration und Benutzer)?

4) Werden die Support-Seiten der Hersteller (Hardware, Betriebssystem und installierte Software) regelmäßig auf Software-Updates und bekannte Schwachstellen geprüft und die Updates eingespielt?

5) Ist auf dem System entsprechende Schutzsoftware (Anti-Virus, Anti-Malware, etc.) installiert, die automatisch E-Mail-Verkehr und Websurfen/Downloads überwacht? Wird diese automatisch aktuell gehalten? Ist diese administrativ für den Standard-Benutzer nicht zugänglich?

6) Ist eine ‚Personal Firewall' installiert und verfügt diese über ein entsprechendes Regelwerk?

7) Wird das Booten von anderen Medien als der primären Festplatte verhindert?

8) Werden sämtliche Nutzerdaten auf einem Server gespeichert? Falls nicht, werden die lokal gespeicherten Daten regelmäßig extern gesichert (z.B. auf einen Firmen-Server, USB-Festplatte, NAS, Cloud, etc.)?

9) Existieren extern gelagerte, aktuelle System-Images, um das System im Bedarfsfall schnell wiederherstellen zu können?

10) Ist die Installation und Verwendung von privater/nicht genehmigter Software unterbunden, insbesondere für Apps auf mobilen Geräten?

11) Sind die Schnittstellen (USB, Firewire, eSATA, etc.) gegen unbefugte Benutzung gesperrt? Wird ein Mißbrauchsversuch protokolliert? Werden Datei-Operationen auf angeschlossene Geräte blockiert und protokolliert?

12) Werden Statusinformationen (Logdateien) gespeichert? Werden die erstellten Berichte regelmäßig auf unberechtigte Zugriffsversuche geprüft?

Zusätzliche Anforderungen für mobile Geräte:

13) Sind die Festplatten und Datenträger verschlüsselt?

14) Ist für die Kommunikation mit dem Firmennetzwerk eine VPN Software installiert? Ist der gleichzeitige Zugriff auf das Firmennetz und das Internet gesperrt? Wird sichergestellt, dass bei Nutzung von WLAN/Hotspots die Kommunikation nur noch über VPN möglich ist?

15) Sind die Kommunikations-Schnittstellen (USB, IrDA, WLAN, Bluetooth, UMTS, etc.) als Standardeinstellung ausgeschaltet?

16) Ist die Möglichkeit der ‚Fernlöschung' aktiviert? Wird wirkungsvoll verhindert, dass die Geräte ‚gejailbreaked' oder ‚gerootet' werden und damit das herstellerseitige Schutzkonzept außer Kraft gesetzt wird?

17) Wird der Bildschirm durch einen Blickschutzfilter vor neugierigen Blicken geschützt?

Sie sind sich in allen Punkten sicher?
Herzlichen Glückwunsch. Sorgen Sie dafür, dass es auch in Zukunft so bleibt. Wir bieten Ihnen mit unseren regelmäßigen Veranstaltungen die Möglichkeit, sich intensiv zu informieren.

Sie haben Fragen oder benötigen Unterstützung?
Kontaktieren Sie uns. Wir beraten und betreuen Sie umfassend, von der Planung über den Betrieb bis zur Störungssuche. Gerne begleiten wir Sie auch durch die entsprechenden Audits.

schuelke.net – internet.security.consulting | Konrad-Adenauer-Strasse 41 | 63225 Langen | www.schuelke.net | +49 (0) 6103 5715571