

Sichere E-Geschäftsprozesse in KMU und Handwerk

Fragebogen 2: Für den Administrator zur Informationssicherheit im Unternehmen

| Nr | Frage | Antwort |
|----|---|---------|
| 1 | Wie werden Daten mit Geschäftspartnern außerhalb Ihres Unternehmens ausgetauscht (E-Mail, ftp, Datenträger, Download, VPN, EDI...)? | |
| 2 | Welche Sicherheitseinrichtungen für die Verbindung zum Internet nach außen sind installiert (Sicherheitgateway, Proxy, Virens Scanner,...)? | |
| 3 | Gibt es für geschäftskritische bzw. rechtlich relevante Daten (Compliance) Möglichkeiten diese zu verschlüsseln und zu signieren? Welche Programme werden genutzt? | |
| 4 | Besteht das Unternehmensnetz aus einem oder mehreren Segmenten? Existiert ein abgesicherter Bereich (DMZ)? | |
| 5 | Werden Gruppenrichtlinien restriktiv durchgesetzt (ja, für kritische Prozesse, nein,...)? | |
| 6 | Erfolgt die Anmeldung über Token und/oder Passwort? In welchen Abständen werden Passwörter geändert? Gibt es Mindestanforderungen an die Passwörter (z. B. 8 Zeichen)? Gibt es eine Passwort-Historie? | |
| 7 | Welche Verfahren zur Sicherung ihrer aktiven Datenbestände setzen Sie ein (RAID, Spiegelung, Tape-Backup, ...)? Werden die Speichermedien sicher verwaltet und gelagert? | |

| | | |
|----|--|--|
| 8 | Welche Medien zur Archivierung der Datenbestände setzen Sie ein (CD/DVD, Bänder, WORM, externe Dienstleister...)? | |
| 9 | Besteht durch Mitarbeiter an den Arbeitsplatzcomputern und Laptops die Möglichkeit Datenträger (Disketten, CD/DVD, USB-Speicherstick,...) ein- und auszulesen? | |
| 10 | Sind auf allen Arbeitsplatzcomputern ständig aktuelle Virens Scanner im Einsatz? Wie oft erfolgt die Aktualisierung? (wöchentlich, monatlich, bei Bedarf)? Besteht ein zentrales Management zur Verteilung der Virensignaturen? | |
| 11 | In welchen Abständen werden durch den Administrator für die genutzte Software Sicherheits-Patches oder - Updates installiert (automatisch, manuell)? | |
| 12 | Ist bei Ausfall des Administrators das Systemwiederanlauf-Szenario dokumentiert? Wurde das geübt? | |
| 13 | Ist die Sicherheit der IT-Systeme auch durch den baulichen Zustand im Unternehmen gesichert (Feuer, Wasser, Einbruch, Kunden, Archiv,...)? Gibt es Problembereiche? | |
| 14 | Welche Protokolle werten Sie aus (Anmeldungen, Firewall, E-Mail-Verkehr, Servermeldungen, ...)? Wie oft werten Sie diese aus (seltener, monatlich, wöchentlich, täglich, bei Bedarf...)? | |
| 15 | Wie schnell können Sie wichtige Hardware bei Defekten ersetzen (Server, Festplatten, Switch,...)? | |

| | | |
|----|---|--|
| 16 | Wie viel Zeit hat der Administrator pro Woche, sich über aktuelle und generelle Fragen der Informationssicherheit weiter zu bilden? Woher erhalten Sie Informationen? (Zeitschriften, Internet, Weiterbildung...) | |
| 17 | Wer schult die Mitarbeiter zur Informationssicherheit? (Administrator, externe Dienstleister, ...) | |
| 18 | Welche Betriebssysteme (Server, Client) sind im Einsatz? Welche Office- und Internetbrowser-Software sind im Einsatz? | |
| 19 | Welche mobilen Komponenten werden im Unternehmen verwendet (WLAN, USB-Geräte, Laptop, Netbook, ...)? | |