KOMPETENZZENTRUM DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Informationssicherheit im Handwerksbetrieb – Vorbeugen und im Ernstfall richtig reagieren

11. November 2019 in Oldenburg

BFE Oldenburg
Bundestechnologiezentrum für
Elektro- und Informationstechnik e.V.

SchmIT-Security, Dipl.-Ing. Werner Schmit

Kurzvorstellung: Dipl.-Ing. Werner Schmit

- Dozent am Bundestechnologiezentrum für Elektro- und Informationstechnik (BFE Oldenburg)
- Arbeitsschwerpunkte
  - Informationssicherheit
  - Datennetzwerktechnik
  - GNU/Linux
  - Systempflege E-Learning-Server
  - Programmierung (C/C++, Java, PHP)

- IT-Security-Beauftragter (TÜV)
- IT-Security-Auditor

- Kontakt
  E-Mail: w.schmit@bfe.de
  Tel.: 0441-34092458

Inhalte

1. Informationssicherheit ist Chefsache
2. Gefahren für Daten, IT-Systeme und Maschinen
3. Erforderliche Maßnahmen für die IT-Sicherheit im Handwerksbetrieb
4. Hinweise für die Umsetzung
5. Fazit

Vortragsziel: Einstieg in das komplexe Themengebiet Informationssicherheit, Sensibilisierung und Orientierung.

Für die konkrete Vorgehensweise zur Entwicklung, Einrichtung und Aufrechterhaltung von Informationssicherheit in Ihrem Handwerksbetrieb gibt es einen separaten Workshop.

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

1. Informationssicherheit ist Chefsache

Blick auf die aktuelle Lage der IT-Sicherheit

WPA2: Forscher entdecken Schwachstelle in WLAN-Verschlüsselung

16. Oktober, 11:02 Uhr 451

Sicherheitsforscher haben offenbar kritische Lücken im Sicherheitsstandard WPA2 entdeckt. Sie geben an, dass sich so Verbindungen belauschen lassen.

heise Security

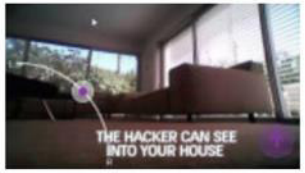
VoIP-Sicherheitslücken

Viele Büro-Telefonanlagen grundlegend unsicher

33 Geräte von 25 Herstellern lassen sich kapern. Angreifer können spionieren, andere Systeme angreifen oder die Organisation durch einen Totalausfall schwächen.

"HomeHack"-Angriff macht aus smarten Staubsaugern Spionage-Tools

26. Oktober, 15:30 Uhr 79



Friedliche Haushaltshelfer im Smart Home können unter bestimmten Voraussetzungen zu fiesen Spionen werden: Ein Proof-of-Concept-Angriff auf eine Steuerungs-App für smarte LG-Geräte offenbarte gravierende Sicherheitsprobleme. Updates stehen bereit.

Was bedeuten die Meldungen für mein Unternehmen?

Die große Verunsicherung ...

- Sind nur größere Unternehmen gefährdet oder bin ich als Kleinbetrieb auch betroffen?
- Wo bin ich gefährdet?
- Was muss ich alles machen, um mich zu schützen?
- Wie gehe ich vor?

IT ist unsicher, aber wir haben Möglichkeiten, uns zu schützen

Viele Wege führen zur Informationssicherheit.
Welcher Weg ist der effektivste?

Quelle: BSI

Kosten und Haftung

- Wieviel kostet mich IT-Sicherheit?
- Muss ich überhaupt etwas tun?
- Reichen 80%-IT-Sicherheit?
- Kann ich mich gegen Schäden versichern?
- Wer haftet im Schadensfall?

IT-Sicherheit ist Chefsache

- Digitalisierung ist ohne IT-Sicherheit nicht möglich. → Grundlage für eine sichere Digitalisierung schaffen.
- Dieses Thema ist so wichtig, dass die Chefin sich selbst darum kümmern muss und es nicht ausschließlich bestimmten Beschäftigten oder externen Dienstleistern überlassen darf.
- Die Chefin muss zumindest so viel davon verstehen, dass sie das Thema managen kann. Um die näheren Einzelheiten können sich dann Experten kümmern.
- Die Chefin ist für die IT-Sicherheit verantwortlich, haftet im Schadensfall.
- Haftung gilt erst recht seit dem 25. Mai 2018 – neue EU-Datenschutzverordnung „der bisher zahnlose Tiger erhält ein Gebiss“

KOMPETENZZENTRUM
DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

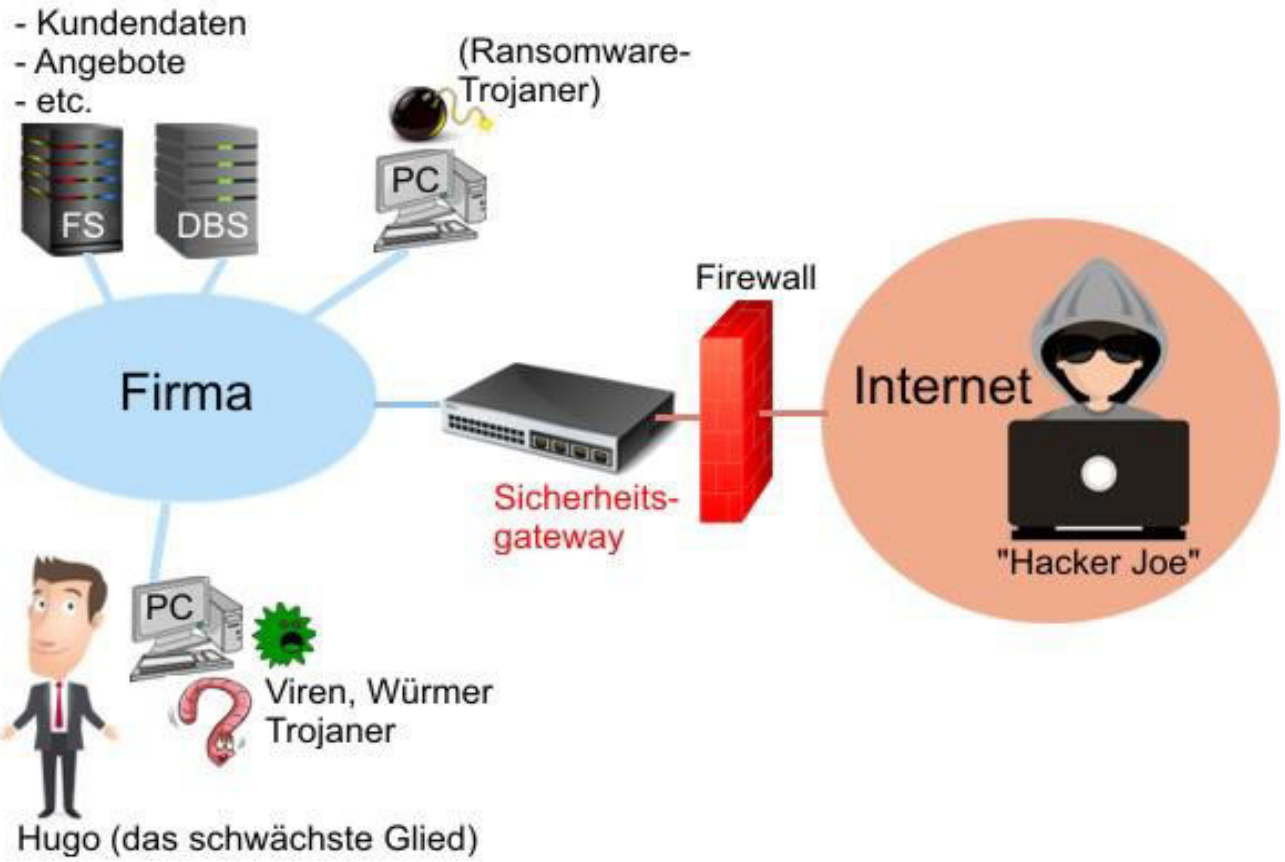
2. Gefahren für Daten, IT-Systeme und Maschinen

„Neulich beim Friseur“

- Friseurbetrieb mit 3 Mitarbeitern
- Räumliche Struktur: Friseursalon ist ein großer Raum mit Raumteiler
- IT-Systeme:
  - 1 x Windows 7-PC als Kassensystem und Universalrechner (E-Mail, Internet, etc.) u. a. mit ...
    - Hypersoft Kassensystemsoftware
    - Microsoft Security Essentials als Virensoftware
    - Teamviewer (für HomeOffice)
    - Thunderbird als E-Mail-Client
    - Weitere Anwendungen (Office, ...) ??
  - 1 x Chef-Notebook (nicht gesehen)
  - 1 x Netzwerkdrucker 1 x DSL-Router (Fritz!Box) mit WLAN-AP
  - Telefonanlage (TK) und VoIP (nicht gesehen)

Gefahren für Daten, IT-Systeme und Maschinen

- Gefahren = a) allgemeine Gefahren (Risiken) und
  b) Sicherheitslücken und Bedrohungen
- Erst, wenn ich die Gefahren kenne, lassen sich erforderliche Maßnahmen daraus herleiten!



Schwachstelle Mensch

- **Social Engineering**
  - Cyberkriminelle setzen zunehmend auf Angriffe, bei denen nicht Schwachstellen in der Software ausgenutzt werden, sondern die Leichtgläubigkeit von Personen. Via Social Engineering können sich Bedrohungen, wie die so genannte Ransomware, rasant verbreiten.

Quelle: heise.de

Mögliche Schäden

- **Sabotage**
  - Verfälschung von Daten
  - Ausfall oder Einschränkung der Funktionsfähigkeit wichtiger IT-Systeme
  - Ausfall, Zerstörung bzw. Manipulation von Maschinen
- **Verlust von Daten**
  - Datenklau
- **Spionage**
  - Kundendaten und andere sensible Unternehmensdaten
    - Forschungs- und Entwicklungsergebnisse, Strategiepapiere, Einzelheiten von Verträgen, Angebote und Preiskalkulationen, die Korrespondenz mit Geschäftspartnern, Informationen über die Besonderheiten der Unternehmens-IT, Zugangsdaten,...
  - Verlust der Vertraulichkeit wichtiger Unternehmensdaten

Mögliche Folgen

- Produktionsverzögerung oder Lieferverzögerungen
- Produktionsausfall
- Auftragsverlust
- Kundenverlust
- spürbare finanzielle Einbußen
- Insolvenz

Kategorisierung der Gefahren

- **Höhere Gewalt**
- **Organisatorische Mängel**
- **Menschliche Fehlhandlungen**
- **Technisches Versagen**
- **Vorsätzliche Handlungen**
- Anmerkung:
  Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat **47 elementare Gefährdungen** ermittelt.

KOMPETENZZENTRUM DIGITALES HANDWERK
BFE OLDENBURG
Mittelstand-Digital
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

3. Erforderliche Maßnahmen für die IT-Sicherheit im Handwerksbetrieb

Unkoordinierte „Insellösungen“ vermeiden

Ein ganzheitliches Sicherheits-konzept ist erforderlich!

Wichtigster Faktor und gleichzeitig größte Schwachstelle ist der Mensch!

Organisatorische Mängel lassen sich nicht mit Technik erschlagen!

Das schwächste Glied in der Kette bestimmt die IT-Sicherheit.

Informationssicherheit und Datenschutz sind fortwährende Prozesse, also nie fertig.

Foto: privat

Informationssicherheit

Sicherheit ist ...

- ... kein Produkt
  - Sicherheit kann man nicht kaufen
  - Sicherheit muss man schaffen
  - Natürlich muss man dazu auf vorhandene Produkte zurückgreifen
- .. kein Projekt
  - Es genügt nicht, Sicherheit einmal zu schaffen
  - Sicherheit muss aufrecht erhalten werden
- ... ein Prozess
  - Kontinuierliche Bearbeitung und Weiterentwicklung erforderlich
- ... Chefsache

Es gibt keine 100%-ige Sicherheit

Bewertung der Informationssicherheit im Betrieb

- Gefahren erkennen
- Risikoanalyse
  - Risiken erfassen, analysieren und bewerten
  - Vollständige Erfassung und adäquate Quantifizierung der bestehenden Risiken
- Behandlung von IT-Risiken → Sicherheitsmaßnahmen definieren
  - Wie gehe ich mit den Risiken um? – Sicherheitsmaßnahmen auf Basis von Kosten, Sicherheitsziele (Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) und Wirksamkeit definieren
    - **ignorieren**
    - **verhindern**
    - **verringern**
    - **versichern**

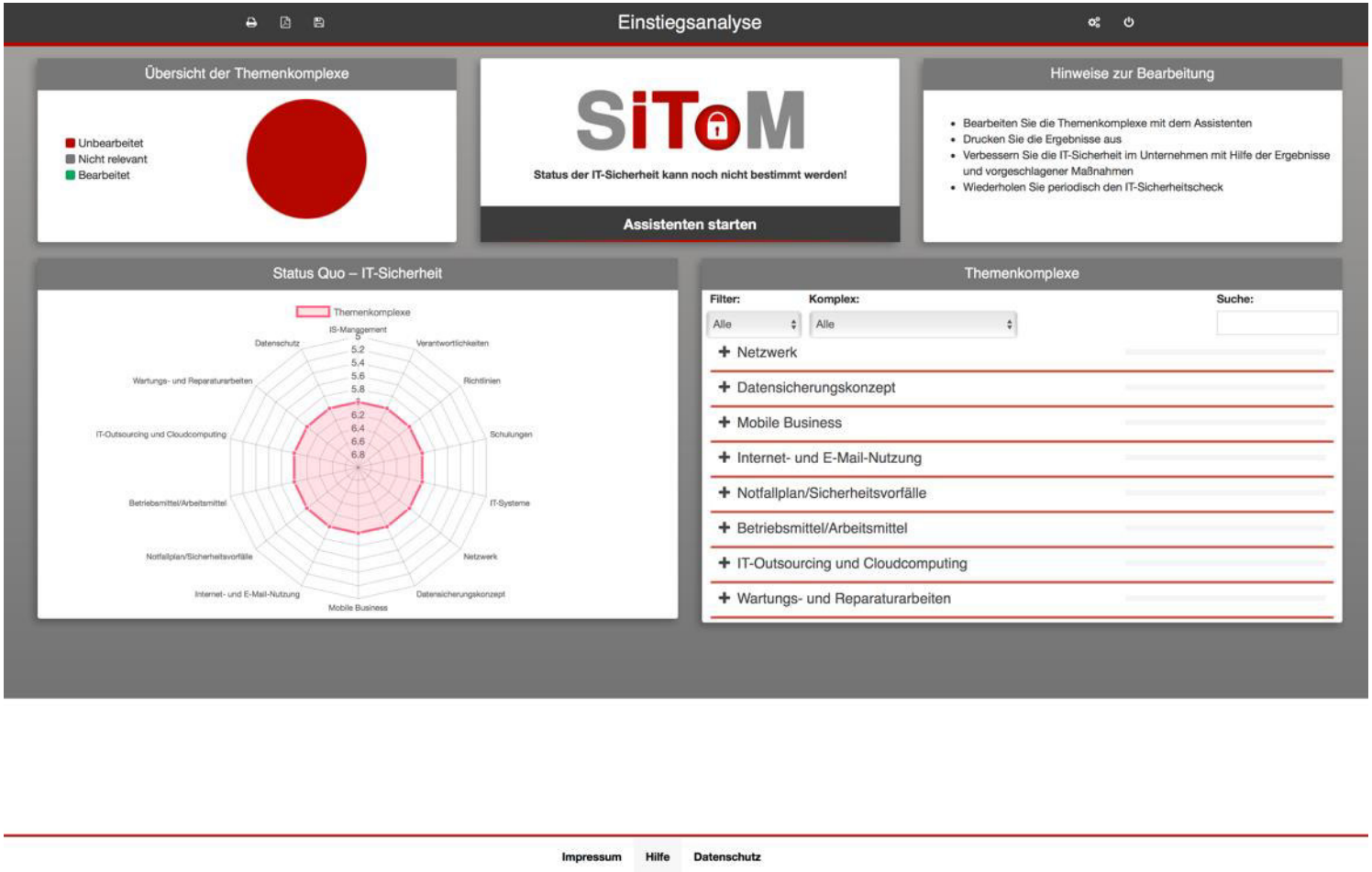
IT-Sicherheitsmaßnahmen nach Kategorien

- **Organisatorische Maßnahmen**
- **Infrastrukturelle Maßnahmen**
- **Personelle Maßnahmen**
- **Technische Maßnahmen**
  - Hard- und Software
  - Kommunikation (Datentransfer)
  - Systempflege
- **Notfallvorsorge und Notfallbewältigung (Notfallmanagement)**

Vorabanalyse - Sicherheitstool Mittelstand (SiToM)

– https://www.sitom.de/home

Status der IT-Sicherheit ermitteln



Organisatorisches -Grundvoraussetzungen

- **„Kronjuwelen“ ermitteln und betrachten**
  - **Überblick über die wichtigsten Daten, Anwendungen und IT-Systeme**
  - Bedrohungen und Risiken erkennen, bewerten und Maßnahmen definieren
  - Wo lauern für mich die Gefahren? Wie hoch ist der mögliche Schaden? Was muss geschützt werden? Was muss ich dagegen tun?

- **Dokumentationen erstellen**
  - Aktuelle Inventarliste der IT-Systeme (Hardware)
  - Liste der installierten Anwendungen (Software)
  - Netzwerkpläne
    - physikalische Netzwerkkonfiguration (Raumplan)
    - logische Netzwerkkonfiguration
  - Checkheft (Serviceheft) von jedem IT-System
    - enthält Konfiguration u. Änderungen

Organisatorische Maßnahmen (1)

- **Zuständigkeiten (Verantwortlichkeiten) festlegen und dokumentieren**
  - Wer ist für die IT-Sicherheit zuständig? → *IT-Sicherheitsbeauftragter*
  - Wer ist für die Systempflege zuständig?
  - Wer führt das Backup durch?
  - Vertretungsregelungen

- **Festlegen, wer sich über die Sicherheitslage informiert**
  - Wichtig!
  - Zum Vergleich: Autofahrer sind ebenfalls verpflichtet, sich über Änderungen von Regeln im Straßenverkehr zu informieren
  - Festlegen, wer sich darum kümmert

- **Einhaltung des Datenschutzes sicherstellen**

Organisatorische Maßnahmen (2)

- **Leitlinie erstellen**

- **Zutritts- / Zugangs- und Zugriffsberechtigungen festlegen und dokumentieren**
  - Berechtigungskonzept - Wer darf was und wo?
  - Rollen und Profile für Benutzer anlegen
  - Zutrittsberechtigungen zu Räumen
  - Zugangsberechtigungen zu IT-Systemen (Anmeldung an einem IT-System)
  - Zugriffsberechtigungen auf Daten und IT-Anwendungen
    - Benutzerrechte
    - need to know-Prinzip (weniger ist mehr)

Organisatorische Maßnahmen (3)

- **Konzept für sichere Netzarchitektur entwickeln und dokumentieren**
  - Betrifft LAN und WLAN
  - Sicherheitszonen bilden → Netzwerksegmentierung
  - z. B. Demilitarisierte Zone (DMZ)
  - Konzept für Sicherheitszonen entwerfen (min 3 nach BSI)
  - Kommunikationskontrolle über Firewalls

- **Firewallkonzept für Ihr Unternehmen entwickeln und umsetzen**
  - Geht nicht ohne “Spezialisten“

- **Checkliste für den Eintritt neuer Mitarbeiter**

- **Checkliste für den Austritt von Mitarbeitern**

Organisatorische Maßnahmen (4)

- **Sicherheitsrichtlinien (engl. Security Policies) erstellen**
  - Richtlinie für Mitarbeiter (u. a. Passwörter, private Nutzung von E-Mail und Internet, Verhalten in sozialen Netzwerken)
  - Richtlinie für Administratoren
  - Richtlinie für den Umgang mit mobilen Datenträgern
  - Richtlinie für den Einsatz von Smartphones

- **Verfahren (Regelungen, Anleitungen, Betriebshandbücher) für Datensicherung, -archivierung und Datenwiederherstellung definieren**

- **Vertraulichkeitsvereinbarungen für Externe oder Mitarbeiter**
  - unterschreiben lassen

- **Sichere Kommunikation mit Kunden und Geschäftspartnern**

Organisatorische Maßnahmen (5)

- **Verfahren für Updates / Patches (Update-/Patch-Management) definieren**
  - Prozess für Patch – und Update Management verankern und dokumentieren
  - Sicherstellen, dass Ihr Betrieb über relevante Updates informiert wird
  - Bezug von Updates aus vertrauenswürdigen Quellen
  - Sicherstellen der Integrität von Updates
  - Durchführen von Tests
  - Freigeben von Updates
  - Zeitnahes Einspielen von Updates

Organisatorische Maßnahmen (6)

- **Merkblätter**
  - Verhalten bei Eintreten eines Virenvorfalls
  - Schutz vor Schadsoftware

- **Listen für den Notfall**
  - Liste mit Passwörtern hinterlegen
  - Liste mit Kontaktdaten hinterlegen
  - Notfallhandbuch
  - Notfallkarte “Verhalten bei IT-Notfällen“

Personelle Maßnahmen (1)

- **Ein- und Austrittsprozess definieren und dokumentieren**
  - Einarbeitung: Geregelte Einarbeitung neuer Mitarbeiter
  - Ausscheiden: Geregelte Verfahrensweise beim Weggang von Mitarbeitern
- **Einweisung im Umgang mit Anwendungen und Systemen**
- **Vertretungsregelungen**
- **Sensibilisierung von Mitarbeitern (Awareness)**
- **Schulung von Mitarbeitern**

Personelle Maßnahmen (2)

- **Regelungen für den Einsatz von Fremdpersonal**
- **Vertraulichkeitsregelungen für den Einsatz von Fremdpersonal**
- **Sicherheitsüberprüfung**
  - Überprüfung von Kandidaten bei der Auswahl von Personal
  - Überprüfung der Vertrauenswürdigkeit von Mitarbeitern
- **Verhalten am Arbeitsplatz**
  - Kann auch über die Richtlinie definiert sein
- **Umgang mit Kennwörtern**

Personelle Maßnahmen (3)

- **Verhalten in sozialen Netzwerken**
- **Umgang mit mobilen Datenträgern**
- **Private Nutzung von E-Mail und Internet**
- **Einsatz von Smartphones**
  - BYOD = Bring Your Own Device

Technische Maßnahmen (1)

- **Datensicherung (Backup) und Archivierung**
  - Konzept erforderlich. Was soll alles gesichert werden? Wie häufig? Wo gespeichert? Wer führt durch? Funktioniert Wiederherstellung? Zurückspeichern testen
  - Regelmäßige Backups sind der einzige Weg, mit dem Anwender und Unternehmen ihre (persönlichen) Daten schützen und im Notfall retten können.
  - **Funktionierendes Backup und Archivierung „leben“**
    - Voraussetzung: Backup- und Archivierungskonzept vorhanden
    - Umsetzung des Verfahrens
    - Tests

Backup

- Gut abgesichert mit der **3-2-1-Regel**
  3 Kopien von jeder wichtigen Datei erstellen, von denen eine lokal und der Rest auf zwei verschiedenen Geräten gespeichert wird.
  Oder: 3 Kopien von jeder Datei, welche auf 2 unterschiedlichen Systemen abgelegt sind, wovon mindestens 1 an einem externen Ort aufbewahrt wird.

- Daten lokal oder extern sichern über Snapshots, Synchronisierung) , zeitgesteuerte Backups und Images

Backup-Strategie

- Adäquate, d. h. dem Handwerksbetrieb und deren „Kronjuwelen“ angepasste, Backup-Strategie erforderlich
- Identifizierung der “Kronjuwelen“
  - Wichtige Daten für den Fortbestand der Firma ermitteln
- Das Backup-Medium darf nicht dauerhaft mit dem zu sichernden Gerät verbunden sein
- Keine Internetanbindung während des Backups – „Offline-Backup“
- Bei kleineren Betrieben zunächst ausreichend, mehrere USB-Festplatten im Wechsel als Backup-Medium anschließen
- Backups erforderlich auch aufgrund rechtlicher Verpflichtung z. B. Datenschutzgesetz
- W-Fragen beantworten, regeln, dokumentieren und umsetzen

Die W-Fragen zur Backup-Strategie

- Welche Daten sollen wie, wie lange und in welchem zeitlichen Abstand gesichert werden?
- Welcher Datenverlust wäre (noch) akzeptabel?
- Welche finanziellen und rechtlichen Konsequenzen drohen bei Verlust der Daten?
- Wann und wie oft müssen die Daten wieder verfügbar sein? (Thema Recovery / Restore)
- Wer ist für die Datensicherung verantwortlich?
- Wie soll die Datensicherung erfolgen?
- Wird die Wiederherstellung der Daten aus dem Backup (regelmäßig) getestet?
- Wo werden die Backups aufbewahrt? – physikalisch getrennte Lagerung zum Schutz bei Brand, Hochwasser oder Diebstahl
- Welche Art der Datenbackupstrategie ist für mich passend?
- Wieviel kostet die Backup-Lösung in der Anschaffung und im laufenden Betrieb?

Technische Maßnahmen (2)

- **Sichere Netzwerkarchitektur implementieren (umsetzen)**
  - Voraussetzung: Konzept dafür vorhanden
  - Umsetzung Sicherheitssegmente (Netzsegmentierung)
  - Firewalls zwischen den Netzsegmenten

- **Sichere stationäre und mobile Endgeräte (Clientsysteme) konfigurieren**
  - Aktuelle Firmware, Betriebssysteme und Anwendungen
  - Personal Firewall
  - Virenscanner
  - Maßnahmen für sicheres Surfen
  - Absicherung und Härtung

Technische Maßnahmen (3)

- **Sichere Server (Serversysteme) konfigurieren**
  - Aktualität
  - Antiviren-Lösung zum Schutz gegen Schadsoftware
  - Personal Firewall
  - Härtung

- **Eindringlingserkennungssysteme (IDS/IPS einsetzen)**
  - Erkennung von Anomalien im Netzwerkverkehr
  - Angriffe gegen Netzwerke oder Computersysteme

- **Netzwerksicherheit - Sicheres Unternehmensnetzwerk (LAN / WLAN) umsetzen**
  - Sichere Funknetze (Absicherung WLAN)
  - Firewalls zwischen Netzsegmenten
  - Unterschiedliche Bewertung bei Office- und ICS-Netz (Produktionsnetz)

Technische Maßnahmen (4)

- **Perimeterschutz = sichere Internetanbindung durch Sicherheitsgateway**
  - Schutz des Firmennetzes nach draußen
  - Mehrstufiges Firewallkonzept erforderlich
  - Sicherheitsgateway verwenden
  - Fritz!Box reicht nicht aus!

- **Sicheren Fernzugriff einrichten (vorher Konzept erstellen!)**
  - Zugriff vom Home Office oder von Baustelle auf Unternehmensressourcen
  - Virtual Private Network (VPN) verwenden
  - Unterschiedliche Bewertung bei Office- und ICS-Netz (Produktionsnetz)

Lösungen für Fernzugriff im Überblick

- (Klassischer) **Fernzugriff über Portweiterleitung**
- **Fernzugriff über die Cloud**
- **Fernzugriff über MyCloud**
- **Fernzugriff über Virtual Private Network (VPN)**
- **Herstellerspezifische Lösungen**

Weitere, für das Handwerk weniger interessant:

- **Fernzugriff über Terminal-Service (TS) oder Virtual Desktop Infrastructure (VDI)**
- **SSH-Tunnel**

Technische Maßnahmen (5)

- **Sichere Konfiguration weiterer eingesetzter Hard- und Software**
  - NAS, Router, WLAN-AP, Webbrowser, ...
- **Monitoring und Logging**
  - Überwachung sowie regelmäßige Kontrolle der Netzwerkkomponenten
  - Aktuellen Netzwerkverkehr beobachten
  - Engpässe und Angriffe erkennen
- **Verschlüsselung der Daten beim Transport und bei der Speicherung**
- **Systempflege (Wartung)**

IT-Systeme im Handwerksbetrieb

- (Windows-)Arbeitsplatzrechner
- Mobile Endgeräte
  - Notebook
  - „Kleingerätezoo“ (Smartphone, Tablet, ...)
- Server
  - Netzwerkspeicher (NAS)
  - Netzdrucker
  - Datenbank-Server
- Managebarer Switch
- WLAN-Access Point
- Sicherheitsgateway (Unternehmensfirewall)
- Router
- TK-Anlage
- ....

Systempflege (1)

- **Update- und Patch Management** → *Sicherheitsupdates, Allgemeine Updates*
  - Betrifft alle IT-Systeme (PCs, Notebooks, „mobiler Kleintierzoo“, Server, Router, Switches, Sicherheitsgateway, IP-Kameras u. sonstige IP-Geräte)
  - zeitnah installieren, Verantwortlichkeiten müssen geklärt sein, …

Systempflege (2)

- **Virenschutz**
  - Erforderlich für sämtliche Endgeräte
  - Empfehlung: kostenpflichtige Produkte wählen
- **Löschen und Vernichten von Daten**
- **Nutzungsanpassungen**
- **Aktuelle Sicherheitsvorgaben** berücksichtigen

Infrastrukturelle Maßnahmen (1)

- Anforderung **Elektrotechnische Verkabelung**
- Anforderung **IT-Verkabelung**
- **Serverräume und IT-Systeme**
  - Schutz gegen Feuer, Überhitzung, Wasserschäden, Überspannung, Stromausfall, Blitzeinschlag und Einbruch
- **Verteilerschrank (**bzw**. Netzwerkschrank)**
  - abschließbar, enthält Patchfeld, Switch, Router

Infrastrukturelle Maßnahmen (2)

- **Zugangs- und Zutrittskontrolle**
  - Für IT-Systeme und Serverräume
  - Nachweisebare Ausgabe von Schlüsseln nur an Berechtigte
  - Authentisierung von Zugriffen
  - Zutrittskontrollsysteme
  - Kontrolle der Aktionen Betriebsfremder

- **Arbeitsplatz**
  - gilt auch für Home Office

Notfallplanung

- **Vorbereitung auf den Sicherheits-Ernstfall**
- Die Frage ist nicht, ob es passiert, sondern wann: Jedes Unternehmen wird irgendwann Opfer von Cyberkriminellen
- Aufbau IT-Notfalldokumentation inklusive Wiederanlauf
- Planung und Durchführung von Notfallübungen
- Eine optimale **Notfallvorsorge** und **Notfallbewältigung** ist nur möglich, wenn geplant und organisiert vorgegangen wird.

Notfallmanagement (1)

- **5 Arten von Ausfällen**, die zu Notfällen führen können
  - Personalausfall (Kennwörter für Server / Tresor-Pin nicht verfügbar, Projektwissen nicht zugänglich)
  - Ausfall von IT-Systemen (Handbuch zum Neustart auf System selbst)
  - Ausfall von Weitverkehrsnetzen (WAN) (kein Telefon / Kein Internet)
  - Ausfall eines Gebäudes (Feuer / Wasserschaden)
  - Ausfall eines Lieferanten oder Dienstleisters

- Professionelles Notfallmanagement reduziert den Schaden und sichert somit den Betrieb und seinen Fortbestand

Notfallmanagement (2)

- Dazu gehören u. a.:
  - **Behandlung von Sicherheitsvorfällen**
  - **Desaster Recovery – Plan**
  - **Notfallkarte und Alarmierungsplan**
  - **Umsetzung Notfallkonzept → Erstellung eines Notfallhandbuchs**
  - **Ersatzsysteme**
  - **Planung Notfallkonzept**
  - **Abläufe, Verzeichnisse mit relevanten Dokumenten und Informationen**
  - **Kontaktlisten mit alternativen Dienstleistern/Lieferanten und Vertretungsregeln**
  - **„Katastrophenschutzübungen“**
    - Wiederanlauf nach einem (Super-)Gau
    - Wiederherstellung vom Backup üben

Gefördert durch:
Bundesministerium
für Wirtschaft
und Energie
aufgrund eines Beschlusses
des Deutschen Bundestages

4. Hinweise für die Umsetzung

Wie organisieren wir die erforderlichen Maßnahmen?

Wir brauchen ein Konzept, eine strukturierte Vorgehensweise, einen Prozess zur Implementierung, Etablierung (Entwicklung und Umsetzung), Aufrechterhaltung und kontinuierlichen Verbesserung von Informationssicherheit im Unternehmen.

→ Ein Qualitätsmanagement (QM) für die IT-Sicherheit
→ Ein durchdachtes Sicherheitskonzept
→ vereinfacht: Wir brauchen einen „**Plan**“
→ Fachbegriff: Informationssicherheits-Managementsystem (**ISMS**)

Ganz nebenbei: **IT-Sicherheit ist ein fortlaufender, nie endender Prozess!!!**

So sieht der „Plan“ aus

Step 1: **Organisatorisches**

- Erforderliche Dokumente erstellen / aktualisieren
- Verantwortlichkeiten festlegen

Step 2: **Erfassung, Analyse und Bewertung**

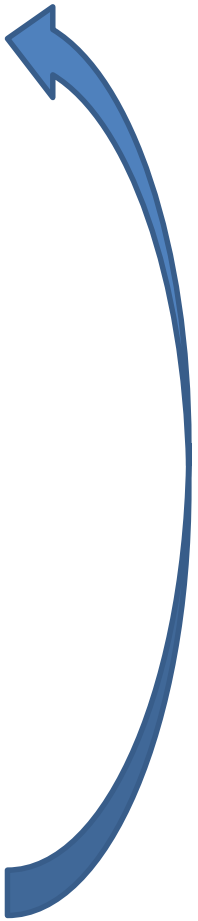
- Erfassung der Daten, Anwendungen und IT-Systeme
- Analyse der Daten, Anwendungen und IT-Struktur
- BSI-Bausteine ermitteln
- Erforderliche Sicherheitsmaßnahmen definieren
- Ist-Soll-Vergleich der Maßnahmen

Step 3: **Implementierung der Sicherheitsmaßnahmen**

- Sicherheitsmaßnahmen umsetzen

Step 4: **Check**

- Kontrolle der Maßnahmen anhand von Checklisten
- Aufrechterhaltung und Verbesserung



Fortsetzung des „Plans“

Dazu immer parallel („täglicher Betrieb“)**:**

- **Sensibilisierung der Mitarbeiter für IT-Sicherheit**
- **Systempflege**
  - **Update- und Patch Management**
  - **Virenschutz**
  - **Datensicherung (Backup) und Archivierung**
  - **...**
- **Notfallvorsorgekonzept und Notfallmanagement (Notfallhandbuch)** (Sicherheitsvorfall / Störung / Ausfall / Notfallvorsorge / Änderung / Kontinuierliche Verbesserung)

ToDo-Liste – Erste Schritte

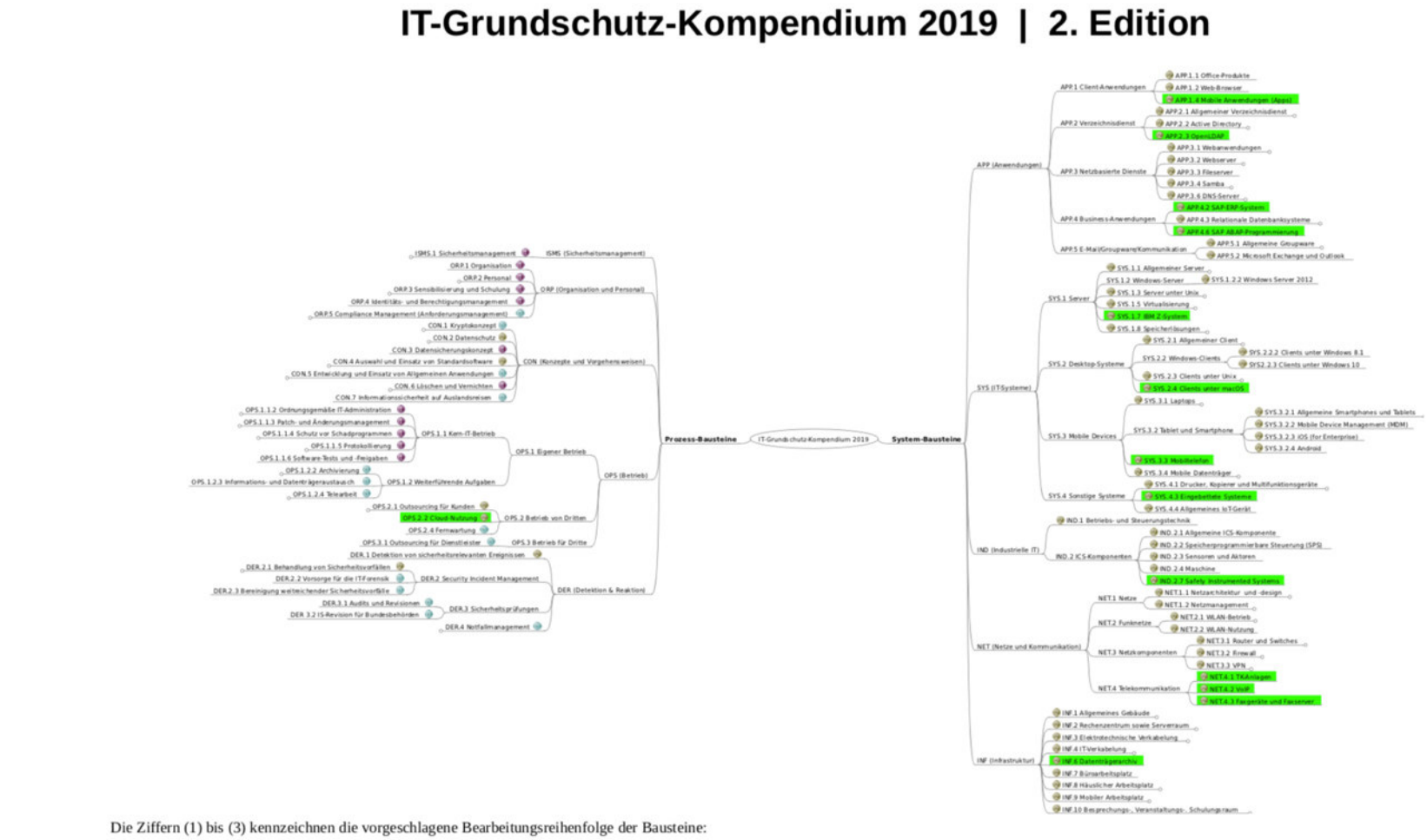
- Stets die Mitarbeiter „mitnehmen“
- Erforderliche Dokumente erstellen
- Sichere Netzwerkarchitektur entwickeln und umsetzen (mehrere Segmente)
- Backup „leben“
- Regelmäßige Systempflege
- Notfallvorsorge / Notfallhandbuch anlegen → *aufbauen*
- Dabei fachkundige Beratung und Unterstützung in Anspruch nehmen!

Unterstützung durch viele Dokumentationen ...

- **Hilfen bei der Umsetzung von Informationssicherheit ...**

BSI ISI-Reihe

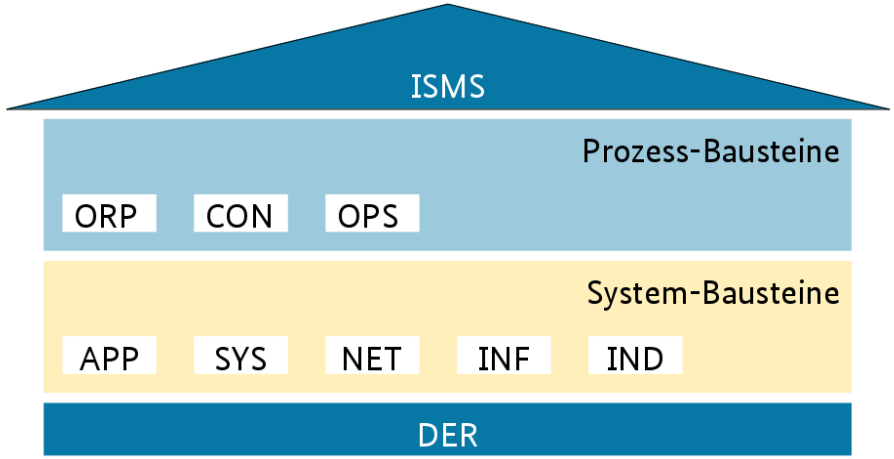
Struktur BSI IT-Grundschutzkompendium



Die Ziffern (1) bis (3) kennzeichnen die vorgeschlagene Bearbeitungsreihenfolge der Bausteine:

IT-Grundschutz Kompendium 2019

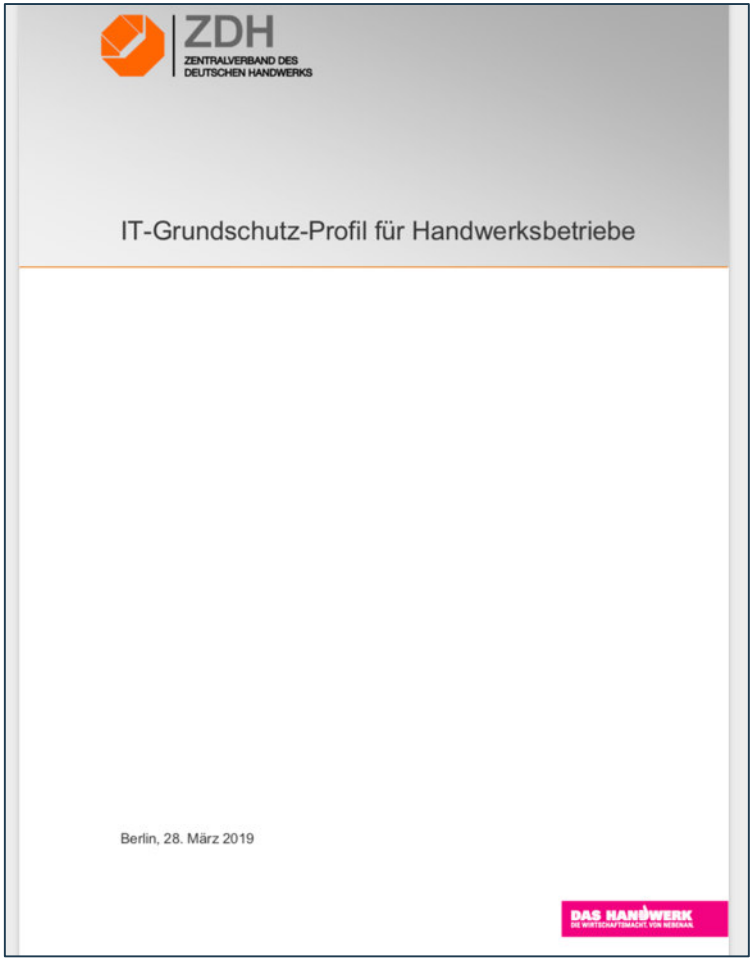
- 840 Seiten
- 94 Bausteine
- Aufbau eines Bausteines:
  - Einführung
  - Basisanforderungen
  - Standardanforderungen
  - Erhöhte Anforderungen



Umsetzungshinweise IT-Grundschutz Kompendium

- nur 1040 Seiten
- nicht für alle Bausteine vorhanden
- Struktur zu einem Baustein
  - 1.Beschreibung
  - 2.Maßnahmen
  - 3.Weiterführende Infos

IT-Grundschutzprofil für Handwerksbetriebe



Routenplaner

Service-Paket „IT-Notfall“
IT-Notfallkarte „Verhalten bei IT-Notfällen“

- 26.09.2019 BSI stellt Service-Paket „IT-Notfall“ vor

Service-Paket „IT-Notfall“
Maßnahmenkatalog zum Notfallmanagement

Allianz für Cyber-Sicherheit

MASSNAHMEN-KATALOG ZUM NOTFALLMANAGEMENT

- Fokus IT-Notfälle -

Um eine ganzheitliche Cyber-Sicherheits-Strategie verfolgen zu können, sollten Sie ein Informations-Sicherheits-Management-System (ISMS) nach anerkannten Standards etablieren. Ein ISMS wird sinnvoll von einem Notfallmanagement/Business Continuity Management (BCM) ergänzt. Dieser Managementprozess obliegt den Notfallbeauftragten und beinhaltet u. a. die Erstellung folgender Produkte:

- einer Leitlinie zum Notfallmanagement,
- Entwicklung eines Notfallvorsorgekonzeptes sowie
- eines Notfallhandbuches.

Service Paket „IT-Notfall“
Top-12-Maßnahmen bei Cyber-Angriffen

Allianz für Cyber-Sicherheit

TOP 12
MASSNAHMEN BEI CYBER-ANGRIFFEN

Diese Fragen sollten Sie sich stellen!

Die Bewältigung eines Cyber-Angriffs ist stets individuell und Maßnahmen müssen auf die Gegebenheiten der IT-Infrastruktur vor Ort, die Art des Angriffs und die Zielsetzungen der Organisation angepasst werden. Die in den 12 als Fragen formulierten Punkten implizierten Maßnahmen dienen als Impuls und Hilfestellung bei der individuellen Bewältigung.

Das Dokument richtet sich an IT-Verantwortliche und Administratoren, in erster Linie in kleinen und mittelständischen Unternehmen.

KDH-Checkliste

- Enthält Prüffragen zu den einzelnen Bereichen der Informationssicherheit
- Umfasst zur Zeit 51 Seiten
- Aus 5 Bereichen
  - Erfassung, Organisation, Allgemeines
  - Infrastruktur
  - Wartung – Allgemein
  - Systempflege IT-Systeme
  - Vorfall, Störung/Ausfall und Kontinuität

Umsetzungshinweise (1)

- **Trotz „Grundschutzprofil für Handwerksbetriebe“ muss jeder Handwerksbetrieb individuell betrachtet werden**
- **Zur „Ermittlung der Kronjuwelen“, Vorgehensweise, Bewertung der IT-Sicherheit, Analyse, etc. ist eine fachliche Begleitung erforderlich**
- **Einige Prozesse sind aus der Umsetzung der EU-Datenschutzrichtlinie bekannt**
- **IT-Grundschutz Kompendium, Umsetzungshinweise zu IT-Grundschutz, ISI-Reihe sind keine esoterische Romane** → Fachchinesisch
- **Eigene Fähigkeiten für IT-Sicherheit realistisch bewerten**
  - KMU: Keine Zeit, Mangelnde Ressourcen, geringes IT-Know How
  - Was kann ich selber machen? Wo hole ich mir Hilfe? Was ist meine Kernkompetenz?

Umsetzungshinweise (2)

- **Richtige „Werkzeuge“ auswählen und auch richtig einsetzen**
  - Werkzeuge für IT-Sicherheit richtig auswählen und richtig einsetzen
  - „Die Werkzeuge sind nur so gut, wie der, der sie anwendet“

- **IT-Security Monitoring erforderlich**
  - Ständige Beobachtung und Analyse des Netzwerkverkehrs
  - Überwachen der verschiedenen Einfallstore für Cyberangreifer
  - Erkennen von Schwachstellen, Frühwarnsysteme

- **Eine vertraglich gesicherte und zyklisch ausgeführte Systempflege wird empfohlen.**

Politisches

- **Gesetzlicher Rahmen für Mindeststandards zur IT-Sicherheit im Kleinunternehmen erforderlich** - Ziel Basisstandard

- **Qualifizierung auf allen Ebenen erforderlich**
  - Unternehmer, Berater, Macher und Prüfer, jeder benötigt mehr oder weniger Grundkenntnisse zur IT-Sicherheit
  - Bildungsangebote zur IT-Sicherheit für das Handwerk auf- bzw. ausbauen
  - Ausbildungsinhalte anpassen

- **Strukturen schaffen**
  - Alle müssen sich noch bewegen und ihre Hausaufgaben machen: Politik, Verbände (HWKs, ZDH,...), Unternehmen – der Handwerksbetrieb, Bildungsanbieter, ??

4. Fazit

Fazit

- Informationssicherheit ist die Voraussetzung für eine erfolgreiche Digitalisierung.
- Informationssicherheit ist ein komplexes Thema.
- Informationssicherheit ist möglich, es gibt allerdings keine 100%-Sicherheit.
- Informationssicherheit bedeutet weit mehr als Firewalls und Virenscanner einsetzen, Router und Switches sicher zu konfigurieren und das WLAN abzusichern.
- Die größte Schwachstelle, „Faktor“ Mensch (der Mitarbeiter), muss einbezogen und überzeugt werden!
- Ein ganzheitlicher Ansatz ist erforderlich.
- **Informationssicherheit ist ein fortlaufender Prozess! Dauerhafte Betreuung, Systempflege und Weiterentwicklung sind erforderlich!**
- **Es gibt viel zu tun. Fangen Sie einfach an.**

Vielen Dank für Ihre Aufmerksamkeit

Version 1.2 vom 14. November 2018

KDH-Checkliste Informationssicherheit für den Handwerksbetrieb

Autor: Dipl.-Ing. Werner Schmit, BFE Oldenburg

Firma: _____

Firma

Erfasst durch: _____

Name / Funktion (z. B.: IT-Sicherheitsbeauftragter)

Erfasst am: _____

Datum

Beteiligte Personen: _____

beteiligte Person

_____

beteiligte Person

Übersicht KDH-Checkliste Informationssicherheit für den Handwerksbetrieb

Bereich 1: Erfassung, Organisation, Allgemeines

1. Organisation - Übergreifende Aspekte
2. Internet-Nutzung
3. Inventarliste der IT-Systeme
4. Netzwerke und Verbindungen
5. Zutritts- , Zugangsberechtigung und Zugriffsrechte
6. Datenschutz
7. Personal

Bereich 2: Infrastruktur

1. Gebäude
2. Elektrotechnische Verkabelung
3. IT-Verkabelung
4. Serverraum
5. Schutzschränke
6. Büroräume u. lokaler Arbeitsplatz
7. Häuslicher Arbeitsplatz (Home Office)

optional: Mobiler Arbeitsplatz / Datenträgerarchiv / Raum für technische Infrastruktur

Bereich 3: Wartung - Allgemein

1. Datensicherung, Datenwiederherstellung und Archivierung
2. Virenschutz

3. Patchmanagement
4. Löschen oder Vernichten von Daten

Bereich 4: Systempflege IT-Systeme

1. Allgemeines
2. Windows-Arbeitsplatzrechner
3. Mobile IT-Systeme (Notebooks)
4. Server
5. Sicherheitsgateway (Unternehmensfirewall)
6. WLAN-Access Points (WLAN-APs)
7. Managebarer Switch
8. NAS
9. Router
10. Mobiler Datenträger
11. Smartphones und Tablets
12. Backup-System (Archivierungssystem)
13. DSL-Router

Bereich 5: Vorfall, Störung/Ausfall und Kontinuität

1. Sicherheitsvorfall
2. Störungen und Ausfälle - Notfallmanagement
3. Änderungen und kontinuierliche Verbesserungen - wiederkehrende Überprüfungen

Bereich 1: Erfassung, Organisation, Allgemeines

1. Organisation -übergreifende Aspekte

2. Internet-Nutzung

3. Inventarliste der IT-Systeme

4. Netzwerke und Verbindungen

5. Zutritt- , Zugangsberechtigung und Zugriffsrechte

6. Datenschutz

7. Personal

Maßnahme	Frage	Umsetzung			Anmerkungen
1.1	**Organisation -Übergreifende Aspekte**				
	Wartungs- und Checkheft für IT-Systeme (IT-Pass)				
	Gibt es ein Checkheft für die IT-Systeme (IT-Pass)?	Ja	teilweise	Nein	
	Enthält das Checkheft die aktuelle Konfiguration, installierte Anwendungen und Daten sowie die Änderungen am System (z. B. durch Einspielen von Sicherheitspatches oder Konfigurationsänderungen)?	Ja	teilweise	Nein	
	Werden Systemänderungen ausreichend und für eine fachkundige Person nachvollziehbar dokumentiert?	Ja	teilweise	Nein	
	Wer ist im Unternehmen für die Checkheftpflege zuständig?	Ja	teilweise	Nein	
	Ist das Checkheft auf aktuellem Stand?	Ja	teilweise	Nein	
	*** Informationssicherheitsbeauftragter (ISB) ***				
	Gibt es im Unternehmen einen Verantwortlichen für Informationssicherheit?	Ja	teilweise	Nein	
	Wer ist das?	Ja	teilweise	Nein	
	Informationssicherheitsleitlinie (IS-Leitlinie)				

	Gibt es im Unternehmen eine gültige Informationssicherheitsleitlinie?	Ja	teilweise	Nein	
	Informationssicherheitsrichtlinien (IS-Richtlinien)				
	Gibt es eine IS-Richtlinie für Nutzer?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie für Administratoren?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie zum Umgang mit mobilen IT-Systemen?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie zum sicheren Umgang mit mobilen Datenträgern?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie für Datensicherung, Datenwiederherstellung und Archivierung?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie zum Umgang mit Störungen und Ausfällen?	Ja	teilweise	Nein	
	Gibt es eine IS-Richtlinie zum Umgang mit Sicherheitsvorfällen?	Ja	teilweise	Nein	
	Gibt es weitere IS-Richtlinien? Welche sind das? (Beispiel: IS-Richtlinie zur Internet-Nutzung, Passwortrichtlinie, IS-Richtlinie zur privaten Nutzung von IT-Systemen, etc.)	Ja	teilweise	Nein	
	*** Sich über die „Sicherheitslage“ informieren ***				
	Gibt es einen Verantwortlichen im Unternehmen, der sich um die aktuelle Sicherheitslage kümmert und entsprechende Maßnahmen zur Umsetzung herleitet?	Ja	teilweise	Nein	
	Gibt es ein Verfahren zur Sicherstellung der Aktualität des Wissens	Ja	teilweise	Nein	
	*** Regelung des Passwortgebrauchs ***				
	Gibt es eine verbindliche Regelung für den Passwortgebrauch (Passwortrichtlinie)?	Ja	teilweise	Nein	
	Sind die Benutzer angewiesen, dem Schutzbedarf angemessene Passwörter mit ausreichender Komplexität zu verwenden?	Ja	teilweise	Nein	
	Sind die Benutzer angewiesen, ihr Passwort geheim zu halten?	Ja	teilweise	Nein	
	Wird getestet, wie viele Stellen des Passwortes tatsächlich vom IT-System überprüft werden?	Ja	teilweise	Nein	
	Werden Passwörter in regelmäßigen Abständen gewechselt? Wie oft erfolgt der Wechsel?	Ja	teilweise	Nein	
	Werden Passwörter sofort gewechselt, sobald sie unautorisierten Personen bekannt geworden sind oder der Verdacht darauf besteht?	Ja	teilweise	Nein	
	Bei erfolglosen Anmeldeversuchen: Wird nicht bekannt gegeben, ob Benutzername und/oder Passwort falsch waren?	Ja	teilweise	Nein	

	*** Hinterlegen des Passwortes ***				
	Ist sichergestellt, dass benannte Vertreter auf die benötigten Anwendungen und IT-Systeme zugreifen können?	Ja	teilweise	Nein	
	Ist geregelt, welche Passwörter hinterlegt werden müssen und welche Sicherheitsvorkehrungen dabei einzuhalten sind?	Ja	teilweise	Nein	
	Wenn Passwörter hinterlegt werden: Werden die Passwörter an einem sicheren Ort hinterlegt?	Ja	teilweise	Nein	
	Wenn Passwörter hinterlegt werden: Werden die hinterlegten Passwörter auf dem aktuellen Stand gehalten?	Ja	teilweise	Nein	
	Wenn Passwörter hinterlegt werden: Wird der Zugriff auf hinterlegte Passwörter dokumentiert?	Ja	teilweise	Nein	

1.2	**Internet-Nutzung**				
	*** IS-Richtlinie zur Internet-Nutzung ***				
	Gibt es eine IS-Richtlinie zur Internet-Nutzung?	Ja	teilweise	Nein	
	Sind alle Mitarbeiter darüber informiert?	Ja	teilweise	Nein	
	*** Sensibilisierung zur sicheren Internet-Nutzung ***				
	Sind die Mitarbeiter über aktuelle Gefahren und Sicherheitsmaßnahmen bei der Internet-Nutzung informiert?	Ja	teilweise	Nein	
	*** Korrektes Auftreten im Internet ***				
	Sind die Mitarbeiter darüber informiert, wie sie im Internet auftreten sollten und welches Verhalten explizit zu vermeiden ist?	Ja	teilweise	Nein	

1.3	**Inventarliste der IT-Systeme**				
	Gibt es eine Regelung zur Inventarisierung der IT-Systeme?	Ja	teilweise	Nein	
	Gibt es eine Inventarliste, in der alle IT-Systeme (inklusive aktive Netzwerkkomponenten) erfasst sind und die zu jedem IT-System ein eindeutiges Identifizierungsmerkmal, Informationen, die eine schnelle Lokalisierung erlauben und Einsatzzweck vermerkt?	Ja	teilweise	Nein	
	Ist die Dokumentation vollständig (ausreichend)?	Ja	teilweise	Nein	

1.4	Netzwerke und Verbindungen				
	Netzwerkdokumentation				
	Gibt es eine Netzwerkdokumentation, die von fachlich versierten Personen verstanden wird und folgende Punkte enthält: aktive Netzwerkkomponenten, Verbindungen untereinander, Verbindungen mit externen Netzwerken, Aufgabe, physikalisches Medium, IT-Systeme und IP-Konfiguration?	Ja	teilweise	Nein	
	Ist diese aktuell und vollständig?	Ja	teilweise	Nein	
	*** Gesicherte Aufstellung aktiver Netzkomponenten ***				
	Werden Netzkomponenten wie Router und Switches in einer gesicherten Umgebung betrieben?	Ja	teilweise	Nein	
	Sind die Passwörter für den Zugriff auf die Konsolen der Netzkomponenten schriftlich an einem sicheren Ort hinterlegt?	Ja	teilweise	Nein	
	Sind Maßnahmen getroffen, um Gefahren durch Beeinträchtigungen der Einsatzumgebung (z. B. Feuchtigkeit, Temperatur), Diebstahl, Vandalismus und unbefugtem Ausschalten der Netzkomponenten vorzubeugen?	Ja	teilweise	Nein	
	Netzübergänge				
	Gibt es eine Netzwerkkopplung ? Welche?	Ja	teilweise	Nein	
	Wenn ja: Erfolgt die Kopplung zu einem internen Netz über einen Router mit Firewall?	Ja	teilweise	Nein	
	Wenn ja: Erfolgt die Anbindung an das öffentliche Netz (Internet) über ein Sicherheitsgateway?	Ja	teilweise	Nein	
	WLAN				
	Gibt es im Unternehmen ein WLAN?	Ja	teilweise	Nein	
	Wenn ja: Sind Sicherheitsmaßnahmen zur Absicherung des WLAN getroffen?	Ja	teilweise	Nein	
	Fernzugriff				
	Erfolgt ein Fernzugriff auf das Netzwerk?	Ja	teilweise	Nein	
	Wozu und ist das dokumentiert?	Ja	teilweise	Nein	
	Wenn Fernzugriff: Wird die Vertraulichkeit, Integrität und Authentizität der übertragenen Informationen geschützt? → MUSS	Ja	teilweise	Nein	
	Wenn Fernzugriff: Ist der Zugriff so gestaltet, dass nur IT-Systeme erreichbar sind, die der jeweilige Nutzer für seine Aufgabenerfüllung benötigt? → MUSS	Ja	teilweise	Nein	
	Wenn Fernzugriff: über eine VPN-Lösung? Welche? Ist die Lösung dokumentiert?	Ja	teilweise	Nein	
		Ja	teilweise	Nein	

1.5	Zutritt- , Zugangsberechtigung und Zugriffsrechte				
	*** IS-Richtlinie (Regelungen) für die Zugriffs- bzw. Zugangskontrolle ***				
	Existieren Regelungen für die Zugangs- und Zugriffskontrolle?	Ja	teilweise	Nein	
	Existieren Standard-Rechteprofile, die den Funktionen und Aufgaben der Nutzer entsprechen?	Ja	teilweise	Nein	
	Existieren schriftliche Zugriffsregelungen sowie eine Dokumentation der Benutzereinrichtung und der Rechtevergabe?	Ja	teilweise	Nein	
	Wird der Zugriff auf alle IT-Systeme und Dienste durch Identifikation und Authentifikation des zugreifenden Benutzers oder IT-Systems abgesichert?	Ja	teilweise	Nein	
	*** Zutrittsregelung und –kontrolle ***				
	Wird der Zutritt zu schutzbedürftigen Gebäudeteilen und Räumen geregelt und kontrolliert?	Ja	teilweise	Nein	
	Existiert ein Konzept für die Zutrittskontrolle?	Ja	teilweise	Nein	
	Werden die Zutrittskontroll-Maßnahmen regelmäßig auf ihre Wirksamkeit überprüft?	Ja	teilweise	Nein	
	*** Vergabe von Zutrittsberechtigungen ***				
	Wurde festgelegt, welche Zutrittsrechte an welche Personen im Rahmen ihrer Funktion vergeben wurden? Liegt eine Dokumentation vor?	Ja	teilweise	Nein	
	Ist die Dokumentation der Zutrittsberechtigungen aktuell und vollständig in Bezug auf schutzbedürftige Räume?	Ja	teilweise	Nein	
	*** Vergabe von Zugangsberechtigungen ***				
	Liegt eine aktuelle Dokumentation über Vergabe sowie Entzug von Zugangsberechtigungen und Zugangsmittel vor?	Ja	teilweise	Nein	
	Orientiert sich die Vergabe von Zugangsberechtigungen an den Funktionen der Zugangsberechtigten?	Ja	teilweise	Nein	
	Werden die Zugangsberechtigten auf den korrekten Umgang mit Zugangsmitteln hingewiesen?	Ja	teilweise	Nein	
	Werden Zugangsberechtigungen bei längerer Abwesenheit von berechtigten Personen vorübergehend gesperrt?	Ja	teilweise	Nein	
	*** Vergabe (Einrichten) von Zugriffsrechten ***				
	Liegt eine aktuelle Dokumentation der vergebenen Zugriffsrechte vor?	Ja	teilweise	Nein	
	Stellt die Konfiguration der IT-Systeme sicher, dass Benutzer nur die Ihnen zugewiesenen Aufgaben erledigen können?	Ja	teilweise	Nein	
	Werden nur die Zugriffsrechte vergeben, die für die jeweiligen Aufgaben erforderlich sind?	Ja	teilweise	Nein	
	Werden beantragte Zugriffsrechte oder Änderungen erteilter Zugriffsrechte von den Verantwortlichen bestätigt und geprüft?	Ja	teilweise	Nein	

	Existiert ein geregeltes Verfahren für den Entzug von Zugriffsrechten?	Ja	teilweise	Nein	
	Wurden Protokollfunktionen, z. B. für erfolglose Anmeldeversuche, unerlaubte Zugriffsversuche sowie Systemfehler aktiviert?	Ja	teilweise	Nein	
	Bei Vertretungslösungen: Wird die Autorisierung des Vertreters vor Erteilung von Zugriffsrechten durch den Administrator geprüft?	Ja	teilweise	Nein	

1.6	**Datenschutz**				
	*** Regelung der Verantwortlichkeiten im Bereich Datenschutz ***				
	Wurde ein Datenschutzbeauftragter bestellt?	Ja	teilweise	Nein	
	Ist der Datenschutzbeauftragte ausreichend qualifiziert?	Ja	teilweise	Nein	
	Stehen dem Datenschutzbeauftragten ausreichend Ressourcen zur Verfügung?	Ja	teilweise	Nein	
	Sind die Aufgaben und Kompetenzen des Datenschutzbeauftragten klar definiert?	Ja	teilweise	Nein	
	*** Prüfung rechtlicher Rahmenbedingungen ***				
	Wird vor der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten geprüft, ob dies erforderlich und rechtlich zulässig ist?	Ja	teilweise	Nein	
	Wird bei allen Geschäftsprozessen und Verfahren darauf geachtet, dass personenbezogene Daten angemessen geschützt sind?	Ja	teilweise	Nein	
	*** technisch-organisatorische Maßnahmen zur Verarbeitung personenbezogener Daten ***				
	Existieren geeignete Vorgaben zum Umgang mit personenbezogenen Daten?	Ja	teilweise	Nein	
	Sind alle technischen und organisatorischen Maßnahmen getroffen, die erforderlich sind, um ausreichenden Datenschutz zu gewährleisten?	Ja	teilweise	Nein	
	*** Verpflichtung / Unterrichtung der Mitarbeiter ***				
	Werden alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet bzw. darüber unterrichtet?	Ja	teilweise	Nein	
	Werden die Mitarbeiter regelmäßig für die Belange des Datenschutzes sensibilisiert?	Ja	teilweise	Nein	
	*** Aufrechterhaltung des Datenschutzes im laufenden Betrieb ***				
	Wird die Einhaltung des datenschutzrechtlichen Anforderungen regelmäßig überprüft?	Ja	teilweise	Nein	
	*** Dokumentation der datenschutzrechtlichen Zulässigkeit ***				
	Wird Hard- und Software, die für die Verarbeitung von personenbezogenen Daten eingesetzt wird, auf die datenschutzrechtliche Zulässigkeit geprüft?	Ja	teilweise	Nein	

	Werden die Prüfergebnisse dokumentiert?	Ja	teilweise	Nein	
	*** Regelung der Auftragsdatenverarbeitung bei der Verarbeitung personenbezogener Daten ***				
	Wurden bei der Vertragsgestaltung zur Auftragsdatenverarbeitung, bei der personenbezogene Daten verarbeitet werden, alle relevanten Datenschutz-Aspekte berücksichtigt?	Ja	teilweise	Nein	
	Ist sichergestellt, das externe Dienstleister die Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden?	Ja	teilweise	Nein	
	Wurden auch beim Auftragnehmer alle Mitarbeiter bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis verpflichtet?	Ja	teilweise	Nein	
	*** Führung von Verfahrensverzeichnissen und Erfüllung der Meldepflichten ***				
	Existiert ein aktuelles Verzeichnis der eingesetzten Hardware, Software und Verfahren sowie der erfassten personenbezogenen Daten?	Ja	teilweise	Nein	
	*** Datenschutzgerechte Löschung / Vernichtung ***				
	Werden Datenträger, die personenbezogene Daten enthalten, sicher gelöscht bzw. vernichtet?	Ja	teilweise	Nein	
	Kontrolliert der Datenschutzbeauftragte regelmäßig, dass Datenträger mit personenbezogenen Daten datenschutzgerecht gelöscht bzw. vernichtet werden?	Ja	teilweise	Nein	

1.7	**Personal**				
	Verfahren				
	Gibt es ein Verfahren zur Aus- und Weiterbildung der Mitarbeiter?	Ja	teilweise	Nein	
	Gibt es ein Verfahren zur Einstellung und Einarbeitung von neuem Personal?	Ja	teilweise	Nein	
	Gibt es ein Verfahren zur Beendigung oder Wechsel eines Arbeitsplatzes	Ja	teilweise	Nein	
	IS-Richtlinien				
	Gibt es IS-Sicherheitsrichtlinien für Nutzer?	Ja	teilweise	Nein	
	Gibt es weitere Nutzer betreffende Richtlinien (z. B. Passwortrichtlinie, Private Nutzung von IT, Nutzung von privater IT (BYOD), IS-Richtlinie zur Internetnutzung)?	Ja	teilweise	Nein	
	Welche weiteren sind das?	Ja	teilweise	Nein	
	Sind alle Mitarbeiter über Regelungen zur Informationssicherheit unterrichtet worden? → MUSS	Ja	teilweise	Nein	
	Sind alle Mitarbeiter darauf hingewiesen worden, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind, solange sie nicht anders gekennzeichnet sind? → MUSS	Ja	teilweise	Nein	
	*** Verpflichtung der Mitarbeiter auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen ***				

	Sind alle Mitarbeiter darauf verpflichtet worden, einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten? → MUSS	Ja	teilweise	Nein	
	Ist den Mitarbeitern bekannt, welcher rechtliche Rahmen ihre Tätigkeit bestimmt?	Ja	teilweise	Nein	
	*** Geregelte Einarbeitung / Einweisung neuer Mitarbeiter***				
	Ist die Einarbeitung von neuem Personal im Bereich der Informationssicherheit geregelt?	Ja	teilweise	Nein	
	Wird jeder neue Mitarbeiter über die relevanten Regelungen zur Informationssicherheit informiert?	Ja	teilweise	Nein	
	*** Schulung vor Programmnutzung ***				
	Werden Mitarbeiter, die eine Aufgabe neu übernehmen sollen, ausreichend geschult?	Ja	teilweise	Nein	
	Werden bei umfangreichen Änderungen in einer IT-Abteilung Schulungsmaßnahmen durchgeführt?	Ja	teilweise	Nein	
	Haben die Mitarbeiter ausreichende Möglichkeiten und Zeit, um sich in neue Aufgaben und Anwendungen einzuarbeiten?	Ja	teilweise	Nein	
	*** Schulung zu Sicherheitsmaßnahmen ***				
	Werden die Mitarbeiter zu Themen rund um die Informationssicherheitsmaßnahmen geschult?	Ja	teilweise	Nein	
	Werden Mitarbeiter regelmäßig zu Themen der Informationssicherheit geschult bzw. sensibilisiert?	Ja	teilweise	Nein	
	Werden Mitarbeiter, die mit personenbezogenen Daten arbeiten, für die gesetzlich erforderlichen Sicherheitsmaßnahmen geschult?	Ja	teilweise	Nein	
	*** Geregelte Verfahrensweise beim Ausscheiden von Mitarbeitern ***				
	Sind die Aktivitäten, die beim Weggang oder Funktionswechsel von Mitarbeitern durchzuführen sind, klar geregelt?	Ja	teilweise	Nein	
	Werden innerhalb des Unternehmens alle betroffenen Stellen über das Ausscheiden des Mitarbeiters informiert? → MUSS	Ja	teilweise	Nein	
	Wird sichergestellt, dass sämtliche Zutrittsrechte, Zugangsberechtigungen und Zugriffsrechte einer ausscheidenden Person entzogen und gelöscht werden? → MUSS	Ja	teilweise	Nein	
	Wird sichergestellt, dass sämtliche unternehmenseigene Werte (z. B. Unterlagen, Ausweise, Schlüssel, Rechner, Speichermedien) einer ausscheidenden Person entzogen und gelöscht werden? → MUSS	Ja	teilweise	Nein	
	Werden dem ausscheidenden Mitarbeiter sämtliche Zugriffsberechtigungen auf IT-Systeme entzogen bzw. diese bei Aufgabenwechsel angepasst? → MUSS	Ja	teilweise	Nein	
	Wird der ausscheidende Mitarbeiter explizit auf Verschwiegenheitsverpflichtungen hingewiesen? → MUSS	Ja	teilweise	Nein	
	Werden bei Ausscheiden eines Mitarbeiters alle Notfall- und andere Ablaufpläne aktualisiert?	Ja	teilweise	Nein	
	*** Vertretungsregelungen ***				
	Existieren in allen Bereichen Vertretungsregelungen?	Ja	teilweise	Nein	
	Wird für die Einführung und Aufrechterhaltung von Vertretungsregelungen Sorge getragen? → MUSS	Ja	teilweise	Nein	

	Ist sichergestellt, dass in Vertretungsfällen ausreichend kompetente Vertreter zur Verfügung stehen?	Ja	teilweise	Nein

Bereich 2: Infrastruktur

1. Gebäude

2. Elektrotechnische Verkabelung

3. IT-Verkabelung

4. Serverraum

5. Schutzschränke

6. Büroräume u. lokaler Arbeitsplatz

7. Häuslicher Arbeitsplatz (Home Office)

optional: Mobiler Arbeitsplatz / Datenträgerarchiv / Raum für technische Infrastruktur

Maßnahme	Frage	Umsetzung			Anmerkungen
2.1	**Gebäude**				
	***Erfassung ***				
	Liegt ein aktueller Infrastrukturplan (Lageplan aller Versorgungsleitungen) vor?	Ja	teilweise	Nein	
	Verfahren				
	Gibt es ein Verfahren zur Absicherung der IT-Systeme und Datenleitungen gegen negative Umwelteinflüsse (z. B. Feuer, Wasser, Staub, Luffeuchtigkeit, etc.)?	Ja	teilweise	Nein	
	Gibt es ein Verfahren für das Anlegen und Ändern von Zugängen und Zutrittsrechten?	Ja	teilweise	Nein	
	*** Geschlossene Fenster und Türen ***				
	Gibt es eine Anweisung, die das Verschließen der Fenster und Außentüren fordert?	Ja	teilweise	Nein	
	Wird regelmäßig überprüft, ob die Fenster und Türen nach Verlassen der Räume verschlossen sind?	Ja	teilweise	Nein	
	*** Gefahrenmeldeanlage ***				
	Gibt es eine den Räumlichkeiten und den Risiken angemessene Gefahrenmeldeanlage?	Ja	teilweise	Nein	
	Wird die Gefahrenmeldeanlage regelmäßig gewartet bzw. geprüft?	Ja	teilweise	Nein	

	Sind die Empfänger von Gefahrenmeldung in der Lage, auf Alarmmeldungen angemessen zu reagieren?	Ja	teilweise	Nein	
	*** Einbruchschutz ***				
	Wurden ausreichende und den örtlichen Gegebenheiten angepasste Maßnahmen zum Einbruchschutz umgesetzt?	Ja	teilweise	Nein	
	Sind die Regelungen zum Einbruchschutz den Mitarbeitern bekannt?	Ja	teilweise	Nein	
	*** Vermeidung von wasserführenden Leitungen ***				
	Sind wasserführende Leitungen in IT-Räumen weitgehend vermieden worden?	Ja	teilweise	Nein	
	Sind Vorkehrungen getroffen worden, um im Notfall einen Wasseraustritt bei wasserführenden Leitungen frühzeitig erkennen zu können?	Ja	teilweise	Nein	
	Werden vorhandene Wasserleitungen an kritischen Stellen durch Sichtkontrolle regelmäßig auf ihre Dichtigkeit hin überprüft?	Ja	teilweise	Nein	
	*** Überspannungsschutz ***				
	Existiert für die USV-Geräte und die IT-Geräte ein Überspannungsschutz?	Ja	teilweise	Nein	
	Werden Blitz- und Überspannungsschutzeinrichtungen periodisch und nach bekannten Ereignissen geprüft und gegebenenfalls ersetzt?	Ja	teilweise	Nein	
	Ist ein durchgängiger Potentialausgleich realisiert?	Ja	teilweise	Nein	
	*** Brandschutz ***				
	Wird sichergestellt, dass Brände (so früh wie möglich) erkannt werden?	Ja	teilweise	Nein	
	Gibt es ausreichend Rauchmelder im Gebäude?	Ja	teilweise	Nein	
	Wird die Funktion der Brandmeldeanlage regelmäßig überprüft?	Ja	teilweise	Nein	
	Gibt es eine speziell für den IT-Bereich zugeschnittene Brandschutzordnung?	Ja	teilweise	Nein	
	Wird regelmäßig kontrolliert, dass die Fluchtwege ohne Hindernisse sind?	Ja	teilweise	Nein	
	*** Brandlastreduzierung ***				
	Wird regelmäßig überprüft, ob sich Brandlasten in den genutzten Räumlichkeiten anhäufen?	Ja	teilweise	Nein	
	Werden unnötige Brandlasten zeitnah entfernt?	Ja	teilweise	Nein	

2.2 Elektrotechnische Verkabelung

	*** Prüfung elektrischer Anlagen ***				
	Werden elektrotechnische Installationen nach der Errichtung durch einen Sachverständigen überprüft?	Ja	teilweise	Nein	
	Wird die elektrotechnische Installation regelmäßig durch einen Sachkundigen auf Betriebssicherheit überprüft?	Ja	teilweise	Nein	

2.3	IT-Verkabelung				
	*** Planung ***				
	Wurden im Rahmen der Planung des Gebäudes und der IT-Verkabelung die einschlägigen Normen wie EN 50310, EN 50173 und EN 50174 berücksichtigt?	Ja	teilweise	Nein	
	*** Fachgerechte Installation ***				
	Ist die IT-Verkabelung unter Einhaltung der gültigen Normen sowie der Herstellervorgaben fachgerecht installiert?	Ja	teilweise	Nein	
	Wird die Verkabelung vor Unterbrechungen, Interferenzen und Schäden geschützt?	Ja	teilweise	Nein	
	Werden Strom- und Datenkommunikationsleitungen getrennt geführt? (Um Interferenzen zu vermeiden)	Ja	teilweise	Nein	
	Werden bei der Auswahl der Kabel die Anforderungen berücksichtigt? (z. B. Schirmung)	Ja	teilweise	Nein	
	Gibt es Pläne der Versorgungsleitungen und der IT-Verkabelung und sind alle Kabel gekennzeichnet und beschriftet?	Ja	teilweise	Nein	
	Wird der Zugang zu Patch-Panels und Verkabelungsräumen kontrolliert?	Ja	teilweise	Nein	
	*** Dokumentation und Kennzeichnung der Verkabelung ***				
	Gibt es einen Verantwortlichen für die Dokumentation der Verkabelung (im Hinblick auf Vollständigkeit, Aktualität und Lesbarkeit)?	Ja	teilweise	Nein	
	Existieren Listen und Bestandspläne mit allen das Netz betreffenden Informationen?	Ja	teilweise	Nein	
	Wird sichergestellt, dass alle Arbeiten an der Verkabelung dem verantwortlichen Mitarbeiter für die Dokumentation rechtzeitig und vollständig mitgeteilt werden?	Ja	teilweise	Nein	
	Wird die Dokumentation der Verkabelung sicher aufbewahrt und der Zugriff entsprechend geregelt?	Ja	teilweise	Nein	
	Werden die Kabel beschriftet, so dass eine Zuordnung der Informationen aus den Bestandsplänen möglich ist?	Ja	teilweise	Nein	
	*** Regelmäßiger Sicherheitscheck des Netzes ***				
	Werden regelmäßige Sicherheitschecks des Netzes, mindestens alle zwei Monate, durchgeführt?	Ja	teilweise	Nein	
	Werden beim Sicherheitscheck alle wichtigen Punkte berücksichtigt?	Ja	teilweise	Nein	

	Werden die Durchführung und die Ergebnisse der Sicherheitschecks dokumentiert?	Ja	teilweise	Nein	
	Wird Abweichungen vom Sollzustand bei Sicherheitschecks nachgegangen und werden weitere Maßnahmen ergriffen?	Ja	teilweise	Nein	

2.4	**Serverraum**				
	*** Erfassung ***				
	Ist ein Serverraum vorhanden?	Ja	teilweise	Nein	
	*** Schutz gegen unbefugten Zutritt ***				
	Werden die Zutritte zu einem Serverraum kontrolliert?	Ja	teilweise	Nein	
	Weisen die Türen, Fenster und Wände der Serverräume einen ausreichenden Einbruch-, Rauch- und Feuerschutz auf?	Ja	teilweise	Nein	
	*** Geeignete Aufstellung von Serversystemen ***				
	Sind die IT-Komponenten in einem gesicherten Raum aufgestellt? (z. B. Ist der Serverraum abschließbar?)	Ja	teilweise	Nein	
	Ist der Zutritt zu den Räumlichkeiten der IT-Komponenten nur berechtigten Personen vorbehalten? (Gibt es eine Zugangsregelung, damit nur Berechtigte Zugang bzw. Zugriff auf den Server haben?)	Ja	teilweise	Nein	
	Ist die Zuverlässigkeit der infrastrukturellen Komponenten sichergestellt? (z. B. durch USV)	Ja	teilweise	Nein	
	**** Klimatisierung der Technik ***				
	Ist Klimatisierung im Serverraum vorhanden?	Ja	teilweise	Nein	
	Werden regelmäßig Wärmelastberechnungen durchgeführt?	Ja	teilweise	Nein	
	Ist sichergestellt, dass die für die IT zulässigen Höchst- und Tiefstwerte für Temperatur und Luftfeuchtigkeit eingehalten werden, z. B. durch eine geeignete Kühlung?	Ja	teilweise	Nein	
	Ist die Kühlung in dem gleichen Maß verfügbar, wie es für die gekühlte IT gefordert wird?	Ja	teilweise	Nein	
	Werden eingesetzte Klimageräte regelmäßig gewartet?	Ja	teilweise	Nein	
	*** Unterbrechungsfreie Stromversorgung ***				
	Ist eine USV vorhanden? (lokale oder zentrale?)	Ja	teilweise	Nein	
	Ist die USV hinsichtlich Leistung und Stützzeit ausreichend dimensioniert?	Ja	teilweise	Nein	
	Wird erneut geprüft, ob die Stützzeit ausreichend ist, wenn Änderungen an den Verbrauchern durchgeführt wurden?	Ja	teilweise	Nein	

	Existiert eine Regelung zum Abschalten und ordnungsgemäßen Herunterfahren von IT-Systemen bei Stromausfall, um Datenverluste zu vermeiden?	Ja	teilweise	Nein	
	Wird die tatsächliche Kapazität der Batterie und damit die Stützzeit der USV regelmäßig getestet?	Ja	teilweise	Nein	
	Werden die Wartungsintervalle der USV eingehalten?	Ja	teilweise	Nein	
	Wird sichergestellt, dass die Batterie im erforderlichen Temperaturbereich gehalten wird?	Ja	teilweise	Nein	

5	**Schutzschränke**				
	*** Erfassung ***				
	Sind Schutzschränke vorhanden? Anzahl?	Ja	teilweise	Nein	
	*** geeignete Aufstellung ***				
	Sind die Schutzschränke so aufgestellt, dass Lüftungsöffnungen frei bleiben und Kabeldurchführungen ohne übergroße Spannungen oder Biegungen möglich sind?	Ja	teilweise	Nein	
	*** Verschluss von Schutzschränken ***				
	Wird darauf geachtet, dass Schutzschränke bei Nichtbenutzung verschlossen werden?	Ja	teilweise	Nein	
	*** gesicherte Aufstellung aktiver Netzkomponenten ***				
	Werden Netzkomponenten wie Router und Switches in einer gesicherten Umgebung betrieben?	Ja	teilweise	Nein	
	Sind die Passwörter für den Zugriff auf die Konsolen der Netzkomponenten schriftlich an einem sicheren Ort hinterlegt?	Ja	teilweise	Nein	
	Sind Maßnahmen getroffen, um Gefahren durch Beeinträchtigungen der Einsatzumgebung (z. B. Feuchtigkeit, Temperatur), Diebstahl, Vandalismus und unbefugtem Ausschalten der Netzkomponenten vorzubeugen?	Ja	teilweise	Nein	
	*** Dimensionierung und Nutzung von Schranksystemen ***				
	Besitzen die Schranksysteme dem Schutzbedarf der darin eingebauten IT-Systeme entsprechende Sicherheitseigenschaften?	Ja	teilweise	Nein	
	Sind die Schutzschränke gegen Feuer, Wasser und Einbruch ausreichend abgesichert?	Ja	teilweise	Nein	
	Sind die eingesetzten Schranksysteme für die Wartbarkeit und Kühlung der darin eingebauten IT-Komponenten geeignet?	Ja	teilweise	Nein	
	Verfügt der Serverschrank über eine ausreichende Klimaanlage?	Ja	teilweise	Nein	
	Verfügt der Serverschrank über eine ausreichende USV-Versorgung?	Ja	teilweise	Nein	
	Einsatz des Schutzschrankes als Serverschrank: Sind zusätzliche Maßnahmen wie Klimatisierung, Not-Aus-Schalter, Überspannungsschutz und USV berücksichtigt worden?	Ja	teilweise	Nein	

2.6	Büroräume u. lokaler Arbeitsplatz				
	**** Abgeschlossene Türen ***				
	Werden Mitarbeiter angewiesen, bei Abwesenheit ihr Büro zu verschließen oder ihre Arbeitsunterlagen wegzuschließen?	Ja	teilweise	Nein	
	Wird sporadisch überprüft, ob Büros beim Verlassen verschlossen werden?	Ja	teilweise	Nein	
	*** Geeignete Aufstellung eines IT-Systems ***				
	Werden IT-Systeme so aufgestellt, dass nur befugte Benutzer die Bildschirminhalte einsehen können?	Ja	teilweise	Nein	
	Werden IT-Systeme so aufgestellt, dass sie von Manipulationen oder Diebstahl geschützt werden?	Ja	teilweise	Nein	
	Werden IT-Systeme so aufgestellt, dass sie vor schädlichen Umwelteinflüssen geschützt werden?	Ja	teilweise	Nein	
	Sind die Benutzer über einen geeigneten Umgang mit IT-Systemen informiert?	Ja	teilweise	Nein	
	*** Geeignete Aufbewahrung dienstlicher Unterlagen und Datenträger ***				
	Werden dienstliche Unterlagen und Datenträger angemessen gesichert?	Ja	teilweise	Nein	
	Stehen an allen Büro-Arbeitsplätzen verschließbare Behältnisse in ausreichender Menge zur Verfügung, um Unterlagen und Datenträger sicher aufbewahren zu können?	Ja	teilweise	Nein	
	Sind die Mitarbeiter darauf hingewiesen worden, dass Unterlagen und Datenträger, die Informationen mit erhöhtem Schutzbedarf enthalten, verschlossen aufzubewahren sind?	Ja	teilweise	Nein	
	**** Der aufgeräumte Arbeitsplatz (ist Organisatorisches) ***				
	Wurden alle Mitarbeiter darauf hingewiesen, dass an unbeaufsichtigten Arbeitsplätzen keine sensiblen Informationen frei zugreifbar sein dürfen?	Ja	teilweise	Nein	
	Werden Arbeitsplätze stichprobenartig kontrolliert, ob schutzbedürftige Informationen offen zugreifbar sind?	Ja	teilweise	Nein	
	*** Ergonomischer Arbeitsplatz ***				
	Sind die Arbeitsplätze aller Mitarbeiter ergonomisch gestaltet?	Ja	teilweise	Nein	
	Ist die Ausrüstung der Computerarbeitsplätze für die möglichst fehlerfreie Bedienung der IT individuell einstellbar?	Ja	teilweise	Nein	
	Sind die am Arbeitsplatz eingesetzten IT-Systeme, vor allem der Bildschirm, ergonomisch und für ungestörtes Arbeiten aufgestellt?	Ja	teilweise	Nein	

2.7	Häuslicher Arbeitsplatz (Home Office)				
	*** geeignete Einrichtung ***				
	Kann der häusliche Arbeitsplatz von den übrigen Wohnbereichen getrennt werden?	Ja	teilweise	Nein	
	Sind an den häuslichen Arbeitsplätzen angemessene Arbeitsmittel und Möbel vorhanden?	Ja	teilweise	Nein	
	Können Unterlagen und IT-Systeme am häuslichen Arbeitsplatz vor unbefugtem Zugriff geschützt werden?	Ja	teilweise	Nein	
	*** Organisation: Akten- und Datenträgertransport zwischen häuslichem Arbeitszimmer und Unternehmen ***				
	Ist geregelt, wie Akten, Datenträger und andere Unterlagen beim Transport zwischen häuslichem Arbeitsplatz und Unternehmen geschützt werden müssen?	Ja	teilweise	Nein	
	Sind Akten, Datenträger und andere Unterlagen ausreichend vor Transportverlusten geschützt?	Ja	teilweise	Nein	
	Sind betroffene Mitarbeiter darüber informiert, wie Akten und Datenträger zu transportieren sind?	Ja	teilweise	Nein	

Bereich 3: Wartung - Allgemein

1. Datensicherung, Datenwiederherstellung und Archivierung

2. Virenschutz

3. Patchmanagement

4. Löschen oder Vernichten von Daten

Maßnahme	Frage	Umsetzung			Anmerkungen
3.1	**Datensicherung, Datenwiederherstellung und Archivierung**				
	IS-Richtlinie und Verfahren				
	Gibt es eine IS-Richtlinie für Datensicherung und Archivierung?	Ja	teilweise	Nein	
	Gibt es ein Verfahren, das die Datensicherung, Datenwiederherstellung und Archivierung definiert?	Ja	teilweise	Nein	
	Gibt es ein Verfahren für Images?	Ja	teilweise	Nein	
	Datensicherung				
	Gibt es ein Datensicherungskonzept (mit Backup-Plan)?	Ja	teilweise	Nein	
	Wer ist dafür verantwortlich?	Ja	teilweise	Nein	
	Archivierung				
	Gibt es ein Archivierungskonzept?	Ja	teilweise	Nein	
	Erfüllt das ausgewählte Archivsystem die im Archivierungskonzept formulierten Anforderungen?	Ja	teilweise	Nein	
	Datenwiederherstellung - Backup-Kontrolle				
	Test: Wird mindestens einmal jährlich sollte ein gesichertes IT-System in einer Testumgebung wiederhergestellt werden, um das Wiederherstellungsverfahren zu testen	Ja	teilweise	Nein	
	Images				

	Gibt es eine Imageverwaltung?	Ja	teilweise	Nein	
	Wird mindestens einmal jährlich der Recovery-Ablauf durch Imagewiederherstellung geprüft?	Ja	teilweise	Nein	
	*** Verwendung geeigneter Archivmedien ***				
	Sind die genutzten Archivmedien für das zu archivierende Datenaufkommen geeignet? (z. B. in Bezug auf das zu archivierende Datenvolumen, mittlere Zugriffszeiten und mittlere gleichzeitige Zugriff auf das Archivsystem)	Ja	teilweise	Nein	
	Sind die genutzten Archivmedien für Langzeitarchivierung (z. B. in Bezug auf Lebensdauer) geeignet?	Ja	teilweise	Nein	
	*** Regelmäßige Funktions- und Recoverytests bei der Archivierung ***				
	Gibt es regelmäßige Funktions- und Recoverytests bei der Archivierung?	Ja	teilweise	Nein	
	Werden Archivierungsdatenträger mindestens einmal jährlich auf Lesbarkeit und Integrität geprüft?	Ja	teilweise	Nein	
	Existiert ein eingespieltes Verfahren, um auf Fehler auf Archivmedien zu reagieren (von Wiederherstellung der Daten bis hin zur sicheren Löschung fehlerhafter Archivmedien)?	Ja	teilweise	Nein	
	Werden alle Hardwarekomponenten des Archivsystems regelmäßig auf ihre einwandfreie Funktion geprüft?	Ja	teilweise	Nein	
	Wird die Fehlerfreiheit aller Archivierungsprozesse einmal pro Tag geprüft?	Ja	teilweise	Nein	
	*** Protokollierung der Archivzugriffe ***				
	Werden Zugriffe auf elektronische Archive protokolliert?	Ja	teilweise	Nein	
	Werden organisationsinterne Regelungen, zum Beispiel zum Datenschutz, bei der Protokollierung von Archivzugriffen beachtet?	Ja	teilweise	Nein	
	Werden zu jedem Zugriff Datum, Uhrzeit, Benutzer, Clientsystem und die ausgeführten Aktionen sowie Fehlermeldungen protokolliert?	Ja	teilweise	Nein	
	Ist die Aufbewahrungsdauer der Protokolldaten im Archivierungskonzept festgelegt?	Ja	teilweise	Nein	
	Werden Protokolldaten von Archivzugriffen unter Beachtung unternehmensinterner Vorgaben regelmäßig ausgewertet?	Ja	teilweise	Nein	

3.2	**Virenschutz**				
	Virenschutzkonzept				

	Verfügen alle IT-Systeme über einen Virenschutz (Schutz vor Schadsoftware)?	Ja	teilweise	Nein	
	Erfolgt eine täglich vollständige Virenüberprüfung jedes IT-Systems?	Ja	teilweise	Nein	
	Verfügen alle IT-Systeme über einen Echtzeitschutz, der alle Dateien, auf die zugegriffen wird, auf Schadsoftware untersucht?	Ja	teilweise	Nein	
	Sucht die Virenschutzsoftware automatisch mindestens einmal täglich nach den neuesten Suchmustern des Herstellers und verwendet diese?	Ja	teilweise	Nein	
	Verhindert die Virenschutzsoftware das Ausführen erkannter Schadsoftware?	Ja	teilweise	Nein	
	Verfahren bei Vorfall				
	Gibt es ein Verfahren zu Reaktionen beim Auftreten eines Sicherheitsvorfalls (Virenbefund)?	Ja	teilweise	Nein	

3.3	**Patchmanagement**				
	*** Informationsbeschaffung über Sicherheitslücken des Systems ***				
	Informieren sich die Administratoren regelmäßig bei verschiedenen Quellen über neu bekannt gewordene Schwachstellen?	Ja	teilweise	Nein	
	Verfahren				
	Gibt es ein Verfahren für das Patchmanagement? Sind Regelungen für das Patchmanagement definiert?	Ja	teilweise	Nein	
	Werden Software-Updates und Patches ausschließlich aus vertrauenswürdigen Quellen bezogen?	Ja	teilweise	Nein	
	Werden Software-Updates und Patches vor dem Roll-Out getestet?	Ja	teilweise	Nein	
	Ist sichergestellt, dass bei einem fehlgeschlagenen Update der ursprüngliche Systemzustand wieder hergestellt werden kann?	Ja	teilweise	Nein	
	Wird die Entscheidung, einen Patch aufgrund aufgetretener Probleme nicht zu installieren, dokumentiert?	Ja	teilweise	Nein	
	*** zeitnahes Einspielen sicherheitsrelevanter Patches und Updates ***				
	Werden sicherheitsrelevanten Updates (Security Patches) zeitnah eingespielt? (Kontrolle im Checkheft)	Ja	teilweise	Nein	
	Bei fehlenden Updates für bekannte Schwachstellen: Werden andere technische oder organisatorische Maßnahmen ergriffen?	Ja	teilweise	Nein	

	*** Zuständigkeit ***				
	Ist geregelt, wer für die Installation der Sicherheitsupdates zuständig ist?	Ja	teilweise	Nein	
	Gibt es eine Vertretungsregelung?	Ja	teilweise	Nein	

3.4	**Löschen oder Vernichten von Daten**				
	*** IS-Richtlinie und Regelungen ***				
	Existiert eine Richtlinie für die Löschung oder Vernichtung von Daten?	Ja	teilweise	Nein	
	Wird die Einhaltung der Richtlinie für die Löschung oder Vernichtung regelmäßig überprüft?	Ja	teilweise	Nein	
	Ist die Richtlinie aktuell? Berücksichtigt sie alle zurzeit eingesetzten Datenträgerarten?	Ja	teilweise	Nein	
	*** Auswahl geeigneter Verfahren ***				
	Wurden für die verschiedenen Datenarten und den jeweiligen Schutzbedarf angemessene Verfahren zum Löschen oder Vernichten festgelegt?	Ja	teilweise	Nein	
	Wurden die Mitarbeiter in die Verfahren zum Löschen oder Vernichten von Informationen eingewiesen, vor allem in den Gebrauch der vorhandenen Werkzeuge und Geräte?	Ja	teilweise	Nein	
	Stehen für die verschiedenen Arten von Datenträgern geeignete Geräte und Werkzeuge zum zuverlässigen Löschen oder Vernichten der gespeicherten Informationen zur Verfügung?	Ja	teilweise	Nein	
	Wird das Ergebnis der Vernichtung regelmäßig kontrolliert?	Ja	teilweise	Nein	
	Ist sichergestellt, dass bei der Löschung von Daten auch die Vorgängerversionen, temporäre Dateien, Dateifragmente oder ähnliches gelöscht werden?	Ja	teilweise	Nein	
	*** Speicher- und Löschfristen ***				
	Sind die Speicher- und Löschfristen für die in dem Unternehmen gespeicherten Informationen bekannt? Werden Sie beachtet?	Ja	teilweise	Nein	
	*** Physikalisches Löschen der Datenträger vor und nach Verwendung ***				
	Stehen den Mitarbeitern Programme zum physikalischen Löschen vor und nach Verwendung von Datenträgern zur Verfügung?	Ja	teilweise	Nein	
	Erfolgt eine physikalische Löschung zuvor anderweitig verwendeter Datenträger vor einem Datenträgertausch?	Ja	teilweise	Nein	

Bereich 4: Systempflege IT-Systeme

1. Allgemeines
2. Windows-Arbeitsplatzrechner
3. Mobile IT-Systeme (Notebooks)
4. Server
5. Sicherheitsgateway (Unternehmensfirewall)
6. WLAN-Access Points (WLAN-APs)
7. Managebarer Switch
8. NAS
9. Router
10. Mobiler Datenträger
11. Smartphones und Tablets
12. Backup-System (Archivierungssystem)
13. DSL-Router

Maßnahme	Frage	Umsetzung			Bemerkung
4.1	**Allgemeines**				
	*** Änderung voreingestellter Passwörter ***				
	Bei Inbetriebnahme: Werden Standardpasswörter durch ausreichend starke Passwörter ersetzt und vordefinierte Logins geändert, bevor IT-Systeme in Betrieb genommen werden?	Ja	teilweise	Nein	
	Bei Inbetriebnahme: Wird geprüft, ob tatsächlich kein Systemzugang mit Standardpasswörtern oder schwachen Passwörtern möglich ist?	Ja	teilweise	Nein	
	*** Lebenszyklus von IT-Systemen ***				
	Inbetriebnahme und Änderung von IT-Systemen				
	Gibt es ein Verfahren, das die Inbetriebnahme und Änderung von IT-Systemen definiert?	Ja	teilweise	Nein	
	Ausmusterung und Wiederverwenden von IT-Systemen				

Gibt es ein Verfahren, das das Ausmustern und Wiederverwenden von IT-Systemen definiert?	Ja	teilweise	Nein	
Entsorgung von (mobilen) Datenträgern				
Gibt es ein Verfahren, das die Entsorgung von (mobilen) Datenträgern definiert?	Ja	teilweise	Nein	
Wer ist für die sichere Entsorgung von Datenträgern zuständig?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.2	**Windows-Arbeitsplatzrechner**				
	Erfassung				
	Welche BIOS-Version?				
	Welche Windows-Version ist installiert?				no go bei Windows XP
	Ist eine Windows-Lizenz vorhanden? Aufbewahrungsort der Lizenz?	Ja	teilweise	Nein	
	Welche Anwendungen sind installiert?				
	Erfolgt die Synchronisierung der Uhrzeit über einen NTP-Server?	Ja	teilweise	Nein	
	Steht der Zeitserver im internen Netz?	Ja	teilweise	Nein	
	Aktualität				
	Ist die BIOS-Firmware auf dem aktuellen Stand?	Ja	teilweise	Nein	
	Ist die Windows-Betriebssystem-Version auf dem aktuellen Stand?	Ja	teilweise	Nein	
	Datum der letzten Aktualisierung	Ja	teilweise	Nein	
	Sind alle Anwendungen auf aktuellem Stand?	Ja	teilweise	Nein	
	Ist Java auf aktuellem Stand?	Ja	teilweise	Nein	
	Sind alle Browser-PlugIns auf aktuellem Stand (kritisch sind: Flash, Java, Adobe Acroread, Silverlight, Quicktime, Active X)?	Ja	teilweise	Nein	
	Ist der Rechner „checkheftgepflegt“, wird regelmäßig gewartet? Sind die Pflegeintervalle dokumentiert?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				

	*** Benutzer- und Passwortschutz für IT-System ***				
	Ist sichergestellt, dass nur berechtigte Personen auf Anwendungen und IT-Systeme zugreifen können?	Ja	teilweise	Nein	
	Ist ein Passwortschutz eingerichtet?	Ja	teilweise	Nein	
	Ist für jeden Nutzer ein Kennwort vergeben?	Ja	teilweise	Nein	
	Verwenden Sie ein nicht zu einfaches Kennwort?	Ja	teilweise	Nein	
	Ist sichergestellt, dass sich die Benutzer mit Name und Kennwort anmelden müssen?	Ja	teilweise	Nein	
	Ist sichergestellt, dass keine automatische Anmeldung am System erfolgt?	Ja	teilweise	Nein	
	**** eingeschränkte Benutzerrechte ***				
	Arbeiten die Nutzer mit eingeschränkten Benutzerrechten(keine Administratorrechte)?	Ja	teilweise	Nein	
	*** Bildschirmsperre ***				
	Ist die manuelle Bildschirmsperre allen Mitarbeitern bekannt und wird diese auch eingesetzt?	Ja	teilweise	Nein	
	Ist eine automatische Bildschirmsperre für jeden Benutzer eingerichtet?	Ja	teilweise	Nein	
	Ist ein Zeitraum für die automatische Bildschirmsperre definiert, der sowohl Nutzer- als auch Sicherheitsbelange berücksichtigt?	Ja	teilweise	Nein	
	*** Sichere Grundkonfiguration ***				
	Wurden nicht benötigte Benutzerkonten, Dienste und Schnittstellen deaktiviert oder entfernt?	Ja	teilweise	Nein	
	Wurde der Server-Dienst deaktiviert, um einen Netzzugriff auf den Arbeitsplatzrechner zu verhindern?	Ja	teilweise	Nein	
	Regelmäßige Prüfung				
	Überprüfen Sie mindestens einmal pro Woche die Aktualität von Betriebssystem, Anwendungen und Browser-Plug-Ins?	Ja	teilweise	Nein	
	Erfolgt eine regelmäßige Prüfung, ob Installation und Konfiguration der Arbeitsplatzrechner den Vorgaben entsprechen?	Ja	teilweise	Nein	
	Werden bei der Kontrolle bzw. Überwachung von Arbeitsplatzrechnern die Bestimmungen zum Datenschutz und zur betrieblichen Mitbestimmung eingehalten?	Ja	teilweise	Nein	
	*** keine automatische Skriptausführung ***				
	Sind Maßnahmen getroffen, die das automatische Ausführen von Skripten (z. B. Java Skript (JS) und Visual Basic(VB)) verhindern?	Ja	teilweise	Nein	
	Welche Maßnahmen sind das?	Ja	teilweise	Nein	
	*** Geeigneter Umgang mit Laufwerken für Wechselmedien und externen Datenspeichern ***				
	Wird verhindert, dass Inhalte von eingelegten Wechseldatenträgern automatisch ausgeführt werden?	Ja	teilweise	Nein	

	Werden technische Maßnahmen ergriffen, um das Booten von anderen als den vorgesehenen Quellen zu verhindern?	Ja	teilweise	Nein	
	Werden technische Maßnahmen ergriffen, um den unautorisierten Anschluss von externen Geräten und Datenträgern zu verhindern?	Ja	teilweise	Nein	
	Werden technische Maßnahmen ergriffen, um den Missbrauch von Wechselmedien zu verhindern?	Ja	teilweise	Nein	
	Existiert eine IS-Richtlinie, die den Umgang mit Wechselmedien und externen Datenspeichern regelt?	Ja	teilweise	Nein	
	Sind die Nutzer über alle Regelungen zum Umgang mit Laufwerken für Wechselmedien und externe Datenspeicher informiert?	Ja	teilweise	Nein	
	*** Virenschutz ***				
	Ist auf allen Arbeitsplatzrechnern ein Viren-Schutzprogramm (Virenscanner-Software mit Echtzeitschutz) installiert?	Ja	teilweise	Nein	
	Welches Produkt?	Ja	teilweise	Nein	
	Verwenden Sie einen Virenscanner, der auch Mails und Dateianhänge überprüft (meist nur in kostenpflichtigen „Suites“ enthalten)?	Ja	teilweise	Nein	
	Wird sichergestellt, dass sowohl Scanprogramm als auch Signaturen stets auf dem aktuellen Stand sind?	Ja	teilweise	Nein	
	Sind die Nutzer mit dem Scanprogramm vertraut, insbesondere mit der Möglichkeit des „On Demand-Scans“?	Ja	teilweise	Nein	
	Wird eine regelmäßige Untersuchung (einmal wöchentlich) des gesamten Datenbestandes auf Schadprogramme durchgeführt?	Ja	teilweise	Nein	
	Wird bei Datenaustausch und Datenübertragung eine Suche nach Schadprogrammen durchgeführt?	Ja	teilweise	Nein	
	Führen Sie regelmäßig einen Komplett-Virenscan über ein Bootmedium (z. B Desinfec’t) durch? Mindestens einmal monatlich? Erfolgt die Dokumentation im Checkheft?	Ja	teilweise	Nein	
	*** Personal Firewall ***				
	Ist auf allen Arbeitsplatzrechnern eine Personal Firewall installiert und aktiviert? Welche?	Ja	teilweise	Nein	
	Wie ist die Personal Firewall konfiguriert?	Ja	teilweise	Nein	
	Datenschutz				
	Sind die Anwender mit eingeschränkten Benutzerrechten angemeldet?	Ja	teilweise	Nein	
	Sind die Daten über Zugriffsrechte gesichert?	Ja	teilweise	Nein	
	Datensicherung und Archivierung				
	Erstellen Sie in regelmäßigen Abständen ein Image des Windows-Arbeitsplatzrechners?	Ja	teilweise	Nein	
	Datum des letzten erstellten Images? Eintrag im Checkheft vorhanden?	Ja	teilweise	Nein	
	Haben Sie in den letzten 6 Monaten das Zurückspeichern des Image (Wiederherstellung) auf einem Testrechner getestet? Wann war das? Eintrag im Checkheft?	Ja	teilweise	Nein	
	Gibt es eine (regelmäßige) Datensicherung des Arbeitsplatzrechners? In welchen Abständen?	Ja	teilweise	Nein	

	Wie erfolgt die Datensicherung auf dem Arbeitsplatzrechner? Was wird gesichert?	Ja	teilweise	Nein	
	Wurde das Zurückspielen von Daten innerhalt des letzten Jahres einmal getestet? Ist dies im Checkheft dokumentiert?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.3	**Mobile IT-Systeme (Notebooks)**				
	Hier gilt die gleiche Checkliste wie beim Arbeitsplatzrechner !!!				
	*** Folgende ERGÄNZUNGEN***				
	IS-Richtlinie und Regelungen für die Nutzung von mobilen IT-Systemen				
	Gibt es eine Informationssicherheits-Richtlinie (**IS-Richtlinie**) zum Umgang mit mobilen IT-Systemen?	Ja	teilweise	Nein	
	Wurden die Benutzer hinsichtlich des Schutzbedarfs mobiler IT-Systeme sowie der darauf befindlichen Daten sensibilisiert?	Ja	teilweise	Nein	
	Wurden die Benutzer hinsichtlich der spezifischen Gefährdungen bzw. entsprechender Maßnahmen bei der Nutzung sensibilisiert?	Ja	teilweise	Nein	
	Sind die Benutzer darüber informiert, welche Art von Informationen auf mobilen IT-Systemen verarbeitet werden dürfen?	Ja	teilweise	Nein	
	*** Zugriffsschutz am Notebook ***				
	Ist ein angemessener Zugriffsschutz für die Notebooks vorhanden?	Ja	teilweise	Nein	
	Verfahren				
	Verlust oder Diebstahl: Gibt es ein Verfahren bei Verlust oder Diebstahl eines mobilen IT-Systems (für Nutzer und Administratoren)?	Ja	teilweise	Nein	
	Gibt es ein Verfahren für die Datensicherung auf mobilen IT-Systemen?	Ja	teilweise	Nein	
	*** weitere Sicherheitsmaßnahmen für Basisschutz***				
	Ist auf dem Notebook ein BIOS-Kennwort vergeben?	Ja	teilweise	Nein	
	Wird über BIOS-Einstellungen oder andere Maßnahmen verhindert, dass das Notebook nicht von externen Datenträgern gestartet werden kann? Durch welche Maßnahme?	Ja	teilweise	Nein	
	Sind die Daten auf der Festplatte verschlüsselt?	Ja	teilweise	Nein	
	Werden Daten und Schlüssel getrennt aufbewahrt?	Ja	teilweise	Nein	
	Wenn ja: Durch eine Hardwareverschlüsselung?	Ja	teilweise	Nein	
	Schutz der Informationen: Sind die auf dem mobilen IT-System gespeicherten Unternehmensdaten vor dem Verlust der Vertraulichkeit und Integrität geschützt?	Ja	teilweise	Nein	

	Regelung Systempflege: Gibt es eine Regelung, wer für die Systempflege zuständig ist?	Ja	teilweise	Nein	
	Datensicherung und Archivierung				
	Gibt es eine Datensicherung?	Ja	teilweise	Nein	
	Was wird gesichert? Wie erfolgt die Datensicherung?	Ja	teilweise	Nein	
	Wo wird das Backup gelagert?	Ja	teilweise	Nein	
	Wer ist für die Datensicherung verantwortlich?	Ja	teilweise	Nein	
	***Diebstahl-Sicherung im mobilen Einsatz ***				
	Verwenden Sie ein Diebstahl-Sicherung im mobilen Einsatz?	Ja	teilweise	Nein	
	*** Nutzung privater mobiler IT-Systeme ***				
	Ist die Nutzung privater mobiler Datenträger und IT-Systeme geregelt?	Ja	teilweise	Nein	
	*** Geeignete Aufbewahrung ***				
	Im mobilen Einsatz: Werden die Benutzer von tragbaren IT-System auf die geeignete Aufbewahrung hingewiesen?	Ja	teilweise	Nein	
	Im stationären Einsatz: Werden tragbare IT-Systeme außerhalb der Nutzungszeiten gegen Diebstahl gesichert bzw. verschlossen aufbewahrt?	Ja	teilweise	Nein	
	Sammelaufbewahrung: Werden nicht im Einsatz befindliche tragbare IT-Systeme von einem unbefugtem Zugriff geschützt?	Ja	teilweise	Nein	
	*** Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen IT-Systemen ***				
	Werden die Mitarbeiter auf den sicheren und sachgerechten Umgang mit mobilen IT-Systemen hingewiesen?	Ja	teilweise	Nein	
	Existieren Vorgaben zur sicheren und sachgerechten Aufbewahrung von mobilen IT-Systemen?	Ja	teilweise	Nein	

Maßnahme	**Frage**	**Umsetzung**			**Bemerkung**
4.4	**Server**				
	Erfassung				
	Welche Aufgabe hat der Server? (Datenbank-/File-/Web-/OwnCloudserver/etc.)?				
	Steht der Server an einem geschützten Standort (Rechnerraum oder Serverschrank)?	Ja	teilweise	Nein	
	Welches Serverbetriebssystem ist installiert? (Linux/Windows/anderes)			Nein	

	Welche Version?				
	Erfolgt die Synchronisierung der Uhrzeit über einen Zeitserver?	Ja	teilweise	Nein	
	Steht der Zeitserver im internen Netz?	Ja	teilweise	Nein	
	Wer ist verantwortlich für die Administration des Servers?				
	Gibt es ein Betriebshandbuch (Checkheft) zum Server?	Ja	teilweise	Nein	
	Ist geregelt, wer Zugriff zum Serverraum bzw. Zugang zum Server hat?	Ja	teilweise	Nein	
	*** IS-Sicherheitsrichtlinie für eine allgemeinen Server ***				
	Gibt es eine IS-Richtlinie für einen allgemeinen Server?	Ja	teilweise	Nein	
	***Sicherheitsmaßnahmen für Basisschutz ***				
	Informiert sich der Systemverantwortliche (Administrator) permanent über den Sicherheitsstatus des Servers und über aktuelle neue Bedrohungen? Nur so können rechtzeitig Gegenmaßnahmen eingeleitet werden.	Ja	teilweise	Nein	
	*** Geeignete Aufstellung ***				
	Steht der Server an einem geeigneten Ort (Serverraum oder Serverschrank)?	Ja	teilweise	Nein	
	*** Restriktive Rechtevergabe ***				
	*** a) Zugriffsrechte ****				
	Sind die Zugriffsrechte auf die auf dem Server gespeicherten Dateien restriktiv vergeben, so dass die Benutzer nur die zur Ausübung ihrer Tätigkeit unbedingt erforderlichen Zugriffsrechte erhalten?	Ja	teilweise	Nein	
	*** b) Zugangsrechte ***				
	Ist der Zugang nur für nutzungsberechtigte Personen geregelt? Systemverwalter (Administrator) hat Zugang zum IT-System und Anwender hat Zugang zur IT-Anwendung?	Ja	teilweise	Nein	
	Erfolgt der Zugang zum IT-System oder IT-Anwendung über eine Identifikation (z. B. Benutzerkennung) und Authentisierung (z. B. Passwort)?	Ja	teilweise	Nein	
	*** Deinstallation nicht benötigter Dienste und Kennungen ***				
	Sind nicht benötigte Dienste deaktiviert bzw. deinstalliert?	Ja	teilweise	Nein	
	Sind nicht benötigte Accounts gesperrt oder gelöscht?	Ja	teilweise	Nein	
	*** Updates und Patches für Betriebssystem und Anwendungen ***				
	Werden zeitnah Sicherheitspatches für Betriebssystem und Anwendungen installiert?	Ja	teilweise	Nein	
	Gibt es ein Verfahren für Updates und Patches?	Ja	teilweise	Nein	
	*** Datensicherung ***				

	Gibt es ein Verfahren zur Datensicherung und Wiederherstellung?	Ja	teilweise	Nein	
	*** Protokollierung ***				
	Ist die Protokollierung auf dem Server aktiviert?	Ja	teilweise	Nein	
	Werden Logdateien erstellt?	Ja	teilweise	Nein	
	Werden die Logdateien regelmäßig ausgewertet?	Ja	teilweise	Nein	
	Wer ist dafür zuständig?	Ja	teilweise	Nein	
	Ist geregelt, wer Zugriff auf die Logdateien hat?	Ja	teilweise	Nein	
	*** Virenschutz ***				
	Ist auf dem Server ein Virenschutzprogramm installiert? Welches?	Ja	teilweise	Nein	
	*** Firewall ***				
	Ist auf dem Server eine Firewall implementiert?	Ja	teilweise	Nein	
	Wenn Firewall: wie ist diese konfiguriert? Gibt es dazu ein Firewallkonzept?	Ja	teilweise	Nein	
	*** Betriebsdokumentation ***				
	Ist die Betriebsdokumentation des Servers aktuell und vollständig? Werden Konfigurationsänderungen dokumentiert?	Ja	teilweise	Nein	
	*** Systemüberwachung ***				
	Erfolgt eine fortlaufende Systemüberwachung? Wie geschieht dies?	Ja	teilweise	Nein	
	Sind weitere Maßnahmen zur Härtung des Betriebssystems getroffen? Welche sind das?	Ja	teilweise	Nein	
	*** Notfallmanagement ***				
	Gibt es ein Notfallmanagement für diesen Server?	Ja	teilweise	Nein	

Maßnahme	**Frage**	**Umsetzung**	**Bemerkung**
5	**Sicherheitsgateway (Unternehmensfirewall)**		
	Erfassung		
	Hersteller und Typ?		

	Welche Firmwareversion ist installiert?				
	Welche Betriebssystemversion ist installiert?				
	Welche Funktionen (Anwendungen, Dienste) sind aktiviert?				
	Wer ist für die Konfiguration zuständig (eigener Mitarbeiter / Systemhaus)?				
	Aktualität				
	Ist die Firmware auf aktuellem Stand? Welche Version?	Ja	teilweise	Nein	
	Ist das Betriebssystem auf aktuellem Stand? Welche Version?	Ja	teilweise	Nein	
	*** IS-Richtlinie für ein Sicherheitsgateway ***				
	Existiert eine Sicherheitsrichtlinie zum Sicherheitsgateway, in der Anforderungen und Vorgaben zum sicheren Betrieb nachvollziehbar dokumentiert sind?	Ja	teilweise	Nein	
	*** Sicherheitsmaßnahmen für Basisschutz***				
	Erfolgt eine sichere Anbindung an die Weboberfläche über https?	Ja	teilweise	Nein	
	Sind komplexe Anmeldekennwörter eingerichtet?	Ja	teilweise	Nein	
	Ist die Fernadministration deaktiviert, also nur der Zugriff auf die Adminoberfläche über die interne (LAN-)Schnittstelle möglich?	Ja	teilweise	Nein	
	*** SPI-Firewall ***				
	Lässt der Paketfilter nur die unbedingt benötigten Kommunikationskanäle offen?	Ja	teilweise	Nein	
	*** Application Level Gateway (ALG) ***				
	Findet eine Filterung der aktiven Inhalte statt?	Ja	teilweise	Nein	
	Findet eine Contenfilterung für den HTTP-Verkehr statt?	Ja	teilweise	Nein	
	Wird der HTTPS-Verkehrt auf Content überprüft?	Ja	teilweise	Nein	
	Wird der Download von Anlagen bzw. Webinhalten mit VBS, Java, Java Script, Active X bzw. CHM (Compiled HTML Modules = Compiled HTML Help) verhindert?	Ja	teilweise	Nein	
	*** Integration von Virenscanner in ein Sicherheitsgateway ***				
	Erfolgt zusätzlich zum dezentralen Virenschutz eine zentrale Filterung auf dem Sicherheitsgateway?	Ja	teilweise	Nein	
	*** NTP-Proxyserver in Sicherheitsgateway ***				
	Dient das Sicherheitsgateway zusätzlich als NTP-Server für die IT-Systeme im Unternehensnetz?	Ja	teilweise	Nein	

	Wird über Firewallregeln bestimmt, dass nur dieser NTP-Server als Zeitserver verwendet werden darf?	Ja	teilweise	Nein	
	*** Integration von VPN-Komponenten in ein Sicherheitsgateway ***				
	Sind VPN-Komponenten so in das Sicherheitsgateway integriert, dass der Datenverkehr wirksam kontrolliert und gefiltert werden kann?	Ja	teilweise	Nein	
	Ist die Entscheidung dokumentiert, wie die VPN-Komponenten in das Sicherheitsgateway zu integrieren sind?	Ja	teilweise	Nein	
	*** Logging und Monitoring ***				
	Werden Änderungen an der Firewallkonfiguration protokolliert (change management)?	Ja	teilweise	Nein	
	*** Datensicherung ***				
	Wird die aktuelle Konfiguration gesichert?	Ja	teilweise	Nein	
	*** Protokollierung der Sicherheitsgateway-Aktivitäten ***				
	Ist festgelegt, welche Ereignisse an den Komponenten des Sicherheitsgateways protokolliert werden?	Ja	teilweise	Nein	
	Erfolgt eine regelmäßige Auswertung der Protokolldateien?	Ja	teilweise	Nein	
	Entspricht die Protokollierung den geltenden datenschutzrechtlichen Bestimmungen?	Ja	teilweise	Nein	
	Erfolgt die Vorhaltung der Protokolldaten zusätzlich zur lokalen Speicherung auf einem zentralen Protokollserver?	Ja	teilweise	Nein	
	Sind die Protokolldaten vor Veränderung geschützt?	Ja	teilweise	Nein	
	Umfasst die Protokollierung an Paketfiltern (SPI-Firewall) mindestens folgende Informationen: Quell- und Ziel-IP-Adresse, Quell- und Zielport oder ICMP-Typ, Datum und Zeit sowie die zutreffende Regel des Paketfilters?	Ja	teilweise	Nein	
	Werden auf dem Application-Level-Gateway (ALG) alle Verbindungen protokolliert?	Ja	teilweise	Nein	
	*** Konzeptentwicklung für das Sicherheitsgateway ***				
	Besteht ein Konzept für das Sicherheitsgateway, das den Einsatzzweck und die Sicherheitsziele erfasst?	Ja	teilweise	Nein	
	Wird die Verwendung des Sicherheitsgateways für die gesamte Netzwerkkommunikation vorgeschrieben?	Ja	teilweise	Nein	
	Sind für die Administration der Komponenten des Sicherheitsgateways ausschließlich gesicherte Zugangsmöglichkeiten vorgesehen?	Ja	teilweise	Nein	
	*** Sicherer Betrieb eines Sicherheitsgateways ***				
	Werden die auf den Sicherheitsgateways umgesetzten Maßnahmen regelmäßig auf ihre Korrektheit überprüft?	Ja	teilweise	Nein	
	Werden Änderungen am Filterregelwerk im Vorfeld auf mögliche sicherheitsrelevante Auswirkungen hin überprüft?	Ja	teilweise	Nein	
	Sind die auf dem Sicherheitsgateway eingesetzten Programme und Dienste auf das erforderliche Maß reduziert?	Ja	teilweise	Nein	

	Werden die an dem Sicherheitsgateway vorgenommenen Einstellung regelmäßig gesichert?	Ja	teilweise	Nein	
	Erfolgt der administrative Zugriff auf die Komponenten des Sicherheitsgateways ausschließlich über vertrauenswürdige Pfade?	Ja	teilweise	Nein	
	*** Festlegung einer Sicherheitsrichtlinie (Policy) für ein Sicherheitsgateway ***				
	Besteht eine Policy für das Sicherheitsgateway, die das Verhalten in Bezug auf Informationen, Dienste und Protokolle definiert und nachvollziehbar dokumentiert?	Ja	teilweise	Nein	
	Ist festgelegt, dass auf dem Sicherheitsgateway ausschließlich zwingend erforderliche Dienste und Programme verfügbar sein dürfen?	Ja	teilweise	Nein	
	Sind Verantwortliche benannt, die für den Entwurf sowie für die Umsetzung und das Testen der Filterregeln zuständig sind?	Ja	teilweise	Nein	
	Sind Gegenmaßnahmen bei erkannten Angriffen gegenüber dem Sicherheitsgateway definiert?	Ja	teilweise	Nein	
	Verfügt das Sicherheitsgateway über Alarmierungsmöglichkeiten für vordefinierte Ereignisse?	Ja	teilweise	Nein	
	Sind die bestehenden Restrisiken bei einem ordnungsgemäßen Betrieb des Sicherheitsgateways bekannt?	Ja	teilweise	Nein	
	*** Integration von Servern in das Sicherheitsgateway ***				
	Sind Maßnahmen umgesetzt, so dass keine weiteren externe Verbindungen unter Umgehung des Sicherheitsgateways geschaffen werden?	Ja	teilweise	Nein	
	Erfolgt der administrative Zugriff auf Informationsserver für externe Benutzer ausschließlich über vertrauenswürdige Pfade?	Ja	teilweise	Nein	
	Wird eine direkte Verbindung der von extern erreichbaren Informationsserver gegenüber dem vertrauenswürdigen Netz verhindert?	Ja	teilweise	Nein	
	Besteht eine netzwerktechnische Trennung der Informationsserver für den internen und externen Bereich?	Ja	teilweise	Nein	
	Sind Informationsserver mit sensiblen Daten für den internen Bereich in einer eigenen DMZ angesiedelt?	Ja	teilweise	Nein	
	*** Einrichtung geeigneter Filterregeln ***				
	Wird für die Filterregeln des Sicherheitgateways das Whitelist-Verfahren angewendet, um alle Verbindungen, die nicht explizit erlaubt werden, zu verbieten?	Ja	teilweise	Nein	
	Werden in den Filterregeln alle Rechner im inneren Netz berücksichtigt?	Ja	teilweise	Nein	
	Sind die eingerichteten Filterregeln des Sicherheitsgateways, z. B. durch Beschreibung der jeweiligen Funktion, dokumentiert?	Ja	teilweise	Nein	
	Werden am Sicherheitsgateway ausschließlich Dienste zugelassen, die den Anforderungen der Sicherheitsrichtlinie entsprechen?	Ja	teilweise	Nein	
	*** Sicherer Betrieb eines Sicherheitsgateways ***				
	Werden die auf den Sicherheitsgateways umgesetzten Maßnahmen regelmäßig auf ihre Korrektheit überprüft?	Ja	teilweise	Nein	
	Werden Änderungen am Filterregelwerk im Vorfeld auf mögliche sicherheitsrelevante Auswirkungen hin überprüft?	Ja	teilweise	Nein	

	Sind die auf dem Sicherheitsgateway eingesetzten Programme und Dienste auf das erforderliche Maß reduziert?	Ja	teilweise	Nein	
	Werden die an dem Sicherheitsgateway vorgenommenen Einstellung regelmäßig gesichert?	Ja	teilweise	Nein	
	Erfolgt der administrative Zugriff auf die Komponenten des Sicherheitsgateways ausschließlich über vertrauenswürdige Pfade?	Ja	teilweise	Nein	
	*** Integration eines Web-Servers in ein Sicherheitsgateway ***				
	hierzu M 5.115 im BSI IT-Grundschutzkatalog beachten	Ja	teilweise	Nein	
	*** Integration eine E-Mail-Servers in ein Sicherheitsgateway ***				
	hierzu M 5.116 im BSI IT-Grundschutzkatalog beachten	Ja	teilweise	Nein	
	*** Integration eines Datenbank-Servers in ein Sicherheitsgateway ***				
	hierzu M 5.117 im BSI IT-Grundschutzkatalog beachten	Ja	teilweise	Nein	
	*** Integration eines DNS-Servers in ein Sicherheitsgateway ***				
	hierzu M 5.118 im BSI IT-Grundschutzkatalog beachten	Ja	teilweise	Nein	
	*** Behandlung von ICMP am Sicherheitsgateway ***				
	hierzu M 5.120 im BSI IT-Grundschutzhandbuch beachten	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.6	**WLAN-Access Points (WLAN-APs)**				
	Erfassung				
	Handelt es sich um einen separaten WLAN-Access-Point (z. B. nicht in einen DSL-Router integriert)?	Ja	teilweise	Nein	
	Welcher Hersteller und Typ?				
	Welche Firmwareversion ist installiert?				
	Welche Verschlüsselung ist eingestellt (WPA1 /WPA2/WPA3)?				
	Wie erfolgt die Authentifizierung (Radius Server / Pre shared key / ...)?				

	Ist ein WLAN-Gastnetz eingerichtet?	Ja	teilweise	Nein	
	Wurde eine Ausleuchtungsmessung durchgeführt, um den Sendebereich des Access Points zu bestimmen?	Ja	teilweise	Nein	
	Existiert eine Sicherung der aktuellen Konfiguration an einem gesicherten Ort?	Ja	teilweise	Nein	
	*** IS-Richtlinie zur WLAN-Nutzung und Regelungen ***				
	Liegt eine Sicherheitsrichtlinie für den Einsatz von WLAN vor?	Ja	teilweise	Nein	
	Ist festgelegt, wer für die Administration der WLAN-Komponenten zuständig ist?	Ja	teilweise	Nein	
	Erfolgt eine regelmäßige Auswertung der Protokolldateien?	Ja	teilweise	Nein	
	Erfolgt eine regelmäßige Prüfung auf unautorisierte WLAN-Komponenten?	Ja	teilweise	Nein	
	Wird die Kenntnisnahme von Anweisungen und Belehrungen durch die WLAN-Benutzer schriftlich bestätigt?	Ja	teilweise	Nein	
	Sind Administratoren und Benutzer über die Sicherheitsrisiken und die zu beachtenden Sicherheitsmaßnahmen im Bereich WLAN informiert?	Ja	teilweise	Nein	
	Ist festgelegt, an welchen internen oder externen Netzen das WLAN gekoppelt werden darf?	Ja	teilweise	Nein	
	Ist ein Prozess mit Handlungsanweisungen bei Sicherheitsproblemen im WLAN-Bereich definiert?	Ja	teilweise	Nein	
	***Wartung**				
	Ist die Firmeware auf aktuellem Stand?	Ja	teilweise	Nein	
	Wann erfolgte die letzte Überprüfung?	Ja	teilweise	Nein	
	Wurde der PSK innerhalb der letzten 3 Monate geändert? Ist das dokumentiert?	Ja	teilweise	Nein	
	Werden die Sicherheitsanforderungen an die eingesetzten WLANs regelmäßig durch Sicherheitsuntersuchungen überprüft?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				
	*** Sicherer Betrieb ***				
	Erfolgt die Administration der WLAN-Komponenten ausschließlich über vertrauenswürdige Pfade?	Ja	teilweise	Nein	
	Sind die Zugriffsmöglichkeiten auf die WLAN-Komponenten auf das erforderliche Maß begrenzt?	Ja	teilweise	Nein	
	Sind die WLAN-Komponenten in das WLAN-Konzept mit einbezogen?	Ja	teilweise	Nein	
	Wird die Verfügbarkeit des Authentisierungsservers über das Management-System erkannt?	Ja	teilweise	Nein	
	Wird der Anschluss fremder WLAN-Access Points oder Manipulationen an bestehenden durch das WLAN-Management-System erkannt?	Ja	teilweise	Nein	
	*** SSID ***				

	Ist die SSID des Access Point so gewählt, dass kein Hinweis auf den Inhaber und den Verwendungszweck gegeben ist?	Ja	teilweise	Nein	
	Ist der SSID-Broadcast deaktiviert?	Ja	teilweise	Nein	
	Konfiguration WLAN-AP				
	Ist WPS deaktiviert?	Ja	teilweise	Nein	
	Ist die korrekte Konfiguration gespeichert und gesichert?	Ja	teilweise	Nein	
	*** Schutz vor unerlaubten physikalischen Zugriff ***				
	Sind die Standardaccounts verändert und ein sicheres Kennwort vergeben?	Ja	teilweise	Nein	
	Ist der Zugriff auf die Admin-Konfigurationsoberfläche des WLAN-AP nur über die LAN-Schnittstelle möglich?	Ja	teilweise	Nein	
	Verschlüsselung				
	Ist als Verschlüsselung nur WPA2 bzw.zukünftig WPA3 eingestellt?	Ja	teilweise	Nein	
	Ist der PSK (Pre shared key), deutsch WLAN-Schlüssel, eine komplexe Zeichenfolge mit mindestens 16 Zeichen?	Ja	teilweise	Nein	
	Wurde das Standard-WLAN-Kennwort des Herstellers(Standard-PSK) geändert?	Ja	teilweise	Nein	
	***WLAN-Absicherung – Sichere Konfiguration ***				
	Ist der DHCP-Server im AP aktiviert	Ja	teilweise	Nein	
	Ist WPS deaktiviert?	Ja	teilweise	Nein	
	Wenn WLAN-Gastnetz: Hat das WLAN-Gastnetz keinen Zugriff auf das Unternehmensnetz?	Ja	teilweise	Nein	
	Wird das WLAN nur dann aktiviert, wenn es benötigt wird (ist eine Zeitsteuerung eingerichtet)?	Ja	teilweise	Nein	
	Werden die Passwörter und Schlüssel (PSK) aller WLAN-Komponenten in regelmäßigen Abständen (mindestens vierteljährlich) gewechselt?	Ja	teilweise	Nein	
	Wann erfolgte die letzte und auch dokumentierte Änderung?	Ja	teilweise	Nein	
	Wurden weitere Maßnahmen zur WLAN-Absicherung getroffen? Welche?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.7	**Managebarer Switch**				
	Erfassung				

	Modell und Hersteller?				
	Welche Firmwareversion?				
	Erfolgt die Synchronisierung der Uhrzeit über einen Zeitserver?	Ja	teilweise	Nein	
	Steht der Zeitserver im internen Netz?	Ja	teilweise	Nein	
	Ist der Einsatzzweck der vorhandenen Switches dokumentiert?	Ja	teilweise	Nein	
	*** Dokumentation der Systemkonfiguration ***				
	Werden Konfigurationsänderungen vom Switch nachvollziehbar dokumentiert?	Ja	teilweise	Nein	
	Werden alle sicherheitsrelevanten Konfigurationen in einem gesonderten Protokoll gespeichert, welches sich nicht auf dem betroffenen Gerät befindet?	Ja	teilweise	Nein	
	Werden die Konfigurationsdateien zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				
	*** Sichere lokale Grundkonfiguration ***				
	Werden für alle eingesetzten Router und Switches Sicherheitspatches durch die Hersteller zur Verfügung gestellt und werden diese eingespielt?	Ja	teilweise	Nein	
	Ist die Firmware auf aktuellem Stand?	Ja	teilweise	Nein	
	Werden für alle eingesetzten Router und Switches die Default-Einstellungen vor dem Einsatz im Produktionsnetz überprüft und mit einer sicheren Grundkonfiguration ausgestattet?	Ja	teilweise	Nein	
	Erfolgt die Grundkonfiguration der Router und Switches offline bzw. nur in einem eigens dafür eingerichteten und besonders gesicherten Testnetz?	Ja	teilweise	Nein	
	Sind die Passwörter der Standardkonten auf den Routern und Switches geändert und entsprechen den Sicherheitsrichtlinien des Unternehmens?	Ja	teilweise	Nein	
	Sind die Standard Accounts geändert bzw. deaktiviert?	Ja	teilweise	Nein	
	Sofern auf den Routern und Switches die Passwörter im Klartext in den Konfigurationsdateien gespeichert werden: Sind die Konfigurationsdateien vor dem unbefugten Zugriff besonders geschützt?	Ja	teilweise	Nein	
	Werden die Passwörter auf den Routern und Switches, sofern möglich, verschlüsselt gespeichert?	Ja	teilweise	Nein	
	Sind Standard-Loginmeldungen auf den Routern und Switches, sofern möglich, durch eine angepasste Version ersetzt, so dass kein Rückschluss auf die eingesetzten Versionen möglich ist?	Ja	teilweise	Nein	
	Sind nicht genutzte Schnittstellen auf Routern und Switches deaktiviert oder einem dafür eingerichteten „Unassigned VLAN“ zugeordnet?	Ja	teilweise	Nein	
	Ist der Zugriff auf die Konfigurationsoberfläche nur aus dem internen Netzwerk möglich?	Ja	teilweise	Nein	
	Ist eine sichere Anmeldung an den managebaren Switches eingerichtet?	Ja	teilweise	Nein	
	Werden Backups der Konfiguration sowohl vor als auch nach der erfolgreichen sicheren Grundkonfiguration durchgeführt?	Ja	teilweise	Nein	
	*** Sichere Netz-Grundkonfiguration von Routern und Switches ***				

	Sind die auf den Routern und Switches zur Verfügung gestellten Dienste auf die benötigten begrenzt?	Ja	teilweise	Nein	
	Ist sichergestellt, dass nur Routing-Protokolle verwendet werden, die eine verschlüsselte Authentisierung unterstützen?	Ja	teilweise	Nein	
	Wird in demilitarisierten Zonen auf den Einsatz von dynamischen Routing-Protokollen verzichtet und werden stattdessen statische Routen genutzt?	Ja	teilweise	Nein	
	Ist sichergesellt, dass das VLAN einer DMZ nicht auf demselben Switch wie das interne Netz konfiguriert ist?	Ja	teilweise	Nein	
	Ist das Spanning Tree Protocol auf den Endgeräte-Ports der Switches deaktiviert?	Ja	teilweise	Nein	
	Ist in der Konfiguration der Switches bei Nutzung des Spanning Tree Protocol eine eindeutig Root-Bridge festgelegt?	Ja	teilweise	Nein	
	Wird, sofern möglich, das VLAN-Pruning eingesetzt, um den Zugriff eines Trunk-Ports auf bestimmte VLANs zu beschränken?	Ja	teilweise	Nein	
	Ist das VLAN-Trunking auf den Engeräte-Ports deaktiviert?	Ja	teilweise	Nein	
	Ist sichergestellt, dass das Default-VLAN nicht für ein produktives VLAN verwendet wird?	Ja	teilweise	Nein	
	Sofern das VLAN Trunking Protocol (VTP) verwendet wird: Wird die von VTP unterstützte Authentisierung verwendet?	Ja	teilweise	Nein	
	Werden zusätzliche Sicherheitsmaßnahmen ergriffen, wenn interne VLANs mit unterschiedlichem Schutzbedarf auf einem Switch konfiguriert sind?	Ja	teilweise	Nein	
	*** Sichere Administration von Routern und Switches ***				
	Erfolgt die Administration der Router und Switches ausschließlich über vertrauenswürdige Pfade?	Ja	teilweise	Nein	
	Sind die Router und Switches in ein zentrales Netzwerkmanagement-System eingebunden?	Ja	teilweise	Nein	
	Ist die Kommunikation für Remote-Zugriffe auf Router und Switches entsprechend abgesichert?	Ja	teilweise	Nein	
	Sind ACLs definiert, die den Zugriff auf das Management-Interface der Router und Switches nur von einer Management-Station erlauben?	Ja	teilweise	Nein	
	*** Sicherung von Switch-Ports (Port Security) ***				
	Erfolgt je nach Schutzbedarf eine port-basierte Zugriffskontrolle auf den Switches?	Ja	teilweise	Nein	
	Sind dauerhaft nicht genutzte Anschlüsse vor unberechtigter Nutzung geschützt (z. B. durch Deaktivierung)?	Ja	teilweise	Nein	
	Erfolgt eine Authentifizierung der angeschlossenen IT-Systeme?	Ja	teilweise	Nein	
	Sind weitere Maßnahmen zur Port Security umgesetzt? Welche?	Ja	teilweise	Nein	
	Access Control Lists				
	Werden Access Control Lists verwendet? (Teil von Port Security)?	Ja	teilweise	Nein	
	*** Wartung und Systempflege ***				
	*** Regelmäßige Kontrolle von Switches ***				

	Wurde ein Kontrollprozess für die Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten etabliert?	Ja	teilweise	Nein	
	*** Software-Pflege ***				
	Sind für das Einspielen von Updates Wartungsfenster festgelegt?	Ja	teilweise	Nein	
	Werden die Updates vor dem produktiven Einsatz getestet?	Ja	teilweise	Nein	
	Erfolgt die Beschaffung der Updates ausschließlich aus vertrauenswürdigen Quellen?	Ja	teilweise	Nein	
	Werden, sofern vom Hersteller angeboten, die Update-Prüfsummen verglichen bzw. die digitalen Signaturen überprüft?	Ja	teilweise	Nein	
	Ist sichergestellt, dass während der Aktualisierung die betroffenen Switches vom produktiven Netz getrennt sind?	Ja	teilweise	Nein	
	*** Protokollierung bei Routern und Switches ***				
	Werden personenbezogene Daten in den Protokolldateien nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet?	Ja	teilweise	Nein	
	Ist der Umfang der Protokollierung und die Kriterien und deren Auswertung dokumentiert und abgestimmt?	Ja	teilweise	Nein	
	Sind Vorgaben definiert, wie eine zeitnahe Auswertung der Protokollinformationen durchzuführen ist?	Ja	teilweise	Nein	
	Werden die Protokollierungsinformationen mit einem korrekten Zeitstempel versehen?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.8	**NAS**				
	Erfassung				
	Hersteller und Typ?				
	Welche Firmwareversion?				
	Welche Betriebssystemversion ist installiert?				
	Welche Anwendungen (Dienste) sind installiert?				
	Fernzugriff: Ist auf dem NAS ein VPN-Server installiert und konfiguriert?	Ja	teilweise	Nein	
	Aktualität				
	Ist die Firmware auf aktuellem Stand?	Ja	teilweise	Nein	
	Ist das Betriebssystem auf aktuellem Stand?	Ja	teilweise	Nein	

	Sind die Anwendungen (Dienste) in der aktuellen Version?	Ja	teilweise	Nein	
	Sind Änderungen und aktuelle Konfiguration im Checkheft hinterlegt?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				
	Ist der Standard-Account geändert (z.B. admin/admin, root/1234)?	Ja	teilweise	Nein	
	Ist ein komplexes Anmeldekennwort eingerichtet?	Ja	teilweise	Nein	
	Welche Dienste sind auf dem NAS aktiviert?	Ja	teilweise	Nein	
	Ist auf dem NAS ein Virenscanner mit Echtzeitschutz installiert und aktiviert?	Ja	teilweise	Nein	
	Wenn ja, welcher?	Ja	teilweise	Nein	
	Ist auf dem NAS eine Firewall aktiviert und konfiguriert?	Ja	teilweise	Nein	
	Wenn ja, welche Konfiguration hat diese?	Ja	teilweise	Nein	
	Sind spezielle Nutzeraccounts mit eingeschränkten Rechten für die Nutzer eingerichtet?	Ja	teilweise	Nein	
	Wenn NAS als VPN-Server: Welche VPN-Technik und welche Sicherheitsmaßnahmen für Zugriffschutz wurden getroffen?	Ja	teilweise	Nein	
	Erfolgt die Synchronisierung der Uhrzeit über einen netzinternen Zeitserver?	Ja	teilweise	Nein	
	Datenschutz				
	Können die Nutzer, nur auf ihre zugewiesenen Verzeichnisse auf der NAS zugreifen?	Ja	teilweise	Nein	
	Erfolgt die Zugriffssteuerung über eingerichtete Benutzerrechte?	Ja	teilweise	Nein	
	Datensicherung				
	Gibt es ein Backup vom NAS auf einem externen Medium?	Ja	teilweise	Nein	
	Liegt das Backup an einem anderen Ort	Ja	teilweise	Nein	
	Wurde in den letzten zwei Monaten das Zurückspielen von Backup-Dateien getestet?	Ja	teilweise	Nein	

Maßnahme	**Frage**	**Umsetzung**	**Bemerkung**
4.9	**Router**		
	Erfassung		

	Modell und Hersteller?				
	Welche Firmwareversion?				
	Erfolgt die Synchronisierung der Uhrzeit über einen Zeitserver?	Ja	teilweise	Nein	
	Steht der Zeitserver im internen Netz?	Ja	teilweise	Nein	
	Ist der Einsatzzweck der vorhandenen Router dokumentiert?	Ja	teilweise	Nein	
	*** Dokumentation der Systemkonfiguration ***				
	Werden Konfigurationsänderungen am Router nachvollziehbar dokumentiert?	Ja	teilweise	Nein	
	Werden alle sicherheitsrelevanten Konfigurationen in einem gesonderten Protokoll gespeichert, welches sich nicht auf dem betroffenen Gerät befindet?	Ja	teilweise	Nein	
	Werden die Konfigurationsdateien zur Notfallvorsorge zusätzlich zentral auf einem dafür vorgesehenen Server gespeichert?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				
	*** Sichere lokale Grundkonfiguration ***				
	Werden für alle eingesetzten Router und Switches Sicherheitspatches durch die Hersteller zur Verfügung gestellt und werden diese eingespielt?	Ja	teilweise	Nein	
	Ist die Firmware auf aktuellem Stand?	Ja	teilweise	Nein	
	Werden für alle eingesetzten Router und Switches die Default-Einstellungen vor dem Einsatz im Produktionsnetz überprüft und mit einer sicheren Grundkonfiguration ausgestattet?	Ja	teilweise	Nein	
	Erfolgt die Grundkonfiguration der Router und Switches offline bzw. nur in einem eigens dafür eingerichteten und besonders gesicherten Testnetz?	Ja	teilweise	Nein	
	Sind die Passwörter der Standardkonten auf den Routern und Switches geändert und entsprechen den Sicherheitsrichtlinien des Unternehmens?	Ja	teilweise	Nein	
	Sind die Standard Accounts geändert bzw. deaktiviert?	Ja	teilweise	Nein	
	Sofern auf den Routern und Switches die Passwörter im Klartext in den Konfigurationsdateien gespeichert werden: Sind die Konfigurationsdateien vor dem unbefugten Zugriff besonders geschützt?	Ja	teilweise	Nein	
	Werden die Passwörter auf den Routern und Switches, sofern möglich, verschlüsselt gespeichert?	Ja	teilweise	Nein	
	Sind Standard-Loginmeldungen auf den Routern und Switches, sofern möglich, durch eine angepasste Version ersetzt, so dass kein Rückschluss auf die eingesetzten Versionen möglich ist?	Ja	teilweise	Nein	
	Sind nicht genutzte Schnittstellen auf Routern und Switches deaktiviert oder einem dafür eingerichteten „Unassigned VLAN“ zugeordnet?	Ja	teilweise	Nein	
	Ist der Zugriff auf die Konfigurationsoberfläche nur aus dem internen Netzwerk möglich?	Ja	teilweise	Nein	
	Ist eine sichere Anmeldung an den managebaren Switch eingerichtet?	Ja	teilweise	Nein	
	Werden Backups der Konfiguration sowohl vor als auch nach der erfolgreichen Grundkonfiguration durchgeführt?	Ja	teilweise	Nein	
	*** Regelmäßige Kontrolle von Routern ***				

	Wurde ein Kontrollprozess für die Sicherstellung des ordnungsgemäßen Betriebs der aktiven Netzkomponenten etabliert?	Ja	teilweise	Nein	
	*** Software-Pflege ***				
	Sind für das Einspielen von Updates Wartungsfenster festgelegt?	Ja	teilweise	Nein	
	Werden die Updates vor dem produktiven Einsatz getestet?	Ja	teilweise	Nein	
	Erfolgt die Beschaffung der Updates ausschließlich aus vertrauenswürdigen Quellen?	Ja	teilweise	Nein	
	Werden, sofern vom Hersteller angeboten, die Update-Prüfsummen verglichen bzw. die digitalen Signaturen überprüft?	Ja	teilweise	Nein	
	Ist sichergestellt, dass während der Aktualisierung die betroffenen Router vom produktiven Netz getrennt sind?	Ja	teilweise	Nein	
	*** Protokollierung bei Routern und Switches ***				
	Werden personenbezogene Daten in den Protokolldateien nur zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebes verwendet?	Ja	teilweise	Nein	
	Ist der Umfang der Protokollierung und die Kriterien und deren Auswertung dokumentiert und abgestimmt?	Ja	teilweise	Nein	
	Sind Vorgaben definiert, wie eine zeitnahe Auswertung der Protokollinformationen durchzuführen ist?	Ja	teilweise	Nein	
	Werden die Protokollierungsinformationen mit einem korrekten Zeitstempel versehen?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.10	**Mobiler Datenträger**				
	Erfassung				
	Art mobiler Datenträger (USB-Stick, externe Festplatte, DVD, etc.)?				
	Hersteller und Typ				
	IS-Richtlinie und Regelungen				
	Gibt es eine IS-Richtlinie zum sicheren Umgang mit mobilen Datenträgern? → MUSS	Ja	teilweise	Nein	
	Gibt es ein Verfahren, wie Nutzer und Administratoren beim Verlust oder Diebstahl eines (kritischen) mobilen Datenträgers vorzugehen haben?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für den Basisschutz				
	Gibt es schriftliche Regeln, die festlegen, ob und wie mobile Datenträger mitgenommen werden dürfen? --> MUSS	Ja	teilweise	Nein	
	Gibt es Sicherheitsmaßnahmen für die Aufbewahrung der mobilen Datenträger?	Ja	teilweise	Nein	

	Gibt es Sicherheitsmaßnahmen zum Virenschutz?	Ja	teilweise	Nein	
	Gibt es Sicherheitsmaßnahmen zur Verschlüsselung der gespeicherten Informationen?	Ja	teilweise	Nein	
	Ist der Verschlüsselungscode (Wiederherstellungscode) an einem dokumentierten Platz hinterlegt?	Ja	teilweise	Nein	
	*** Sensibilisierung der Mitarbeiter zum sicheren Umgang mit mobilen Datenträgern ***				
	Werden die Mitarbeiter auf den sicheren und sachgerechten Umgang mit mobilen IT-Systemen hingewiesen?	Ja	teilweise	Nein	
	Sind die Mitarbeiter zum sicheren Umfang mit mobilen Datenträgern sensibilisiert? → MUSS	Ja	teilweise	Nein	
	Existieren Vorgaben zur sicheren und sachgerechten Aufbewahrung von mobilen IT-Systemen?	Ja	teilweise	Nein	
	*** Verlustmeldung mobiler Datenträger ***				
	Ist klar geregelt, dass der Verlust mobiler Datenträger umgehend gemeldet wird? Dies umfasst auch private Datenträger, die dienstlich genutzt werden. → MUSS	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.11	**Smartphones und Tablets**				
	Erfassung				
	Hersteller und Typ?				
	Welche Betriebssystemversion?				
	Welche Anwendungen sind installiert?				
	Ist im Unternehmen ein MDM (Mobile Device Management) für Smartphones bzw. Tablets implementiert?	Ja	teilweise	Nein	
	Aktualität				
	Ist das Betriebssystem auf dem aktuellen Stand?	Ja	teilweise	Nein	
	Sind die Anwendungen aktuell?	Ja	teilweise	Nein	
	*** IS-Richtlinie zum Umgang mit Smartphones ***				
	Gibt es eine IS-Richtlinie zum Umgang mit Smartphones?	Ja	teilweise	Nein	
	Wie wird die Einhaltung der IS-Richtlinie überprüft?	Ja	teilweise	Nein	
	Besitzt jeder Smartphone-Benutzer ein Exemplar dieser IS-Richtlinie oder ein Merkblatt mit einem Überblick über die wichtigsten Sicherheitsmechanismen?	Ja	teilweise	Nein	

	Sicherheitsmaßnahmen für Basisschutz				
	*** Konfiguration ***				
	Sind beim Smartphone alle nicht benötigten Schnittstellen deaktiviert?	Ja	teilweise	Nein	
	Sind alle nicht benötigten Anwendungen deinstalliert worden?	Ja	teilweise	Nein	
	Werden die Smartphones zentral administriert?	Ja	teilweise	Nein	
	Wird der Zugriff auf das Smartphone durch eine Authentisierung geschützt? Gibt es einen Zugangsschutz?	Ja	teilweise	Nein	
	Sind über ein Rechtemanagement (Rechte der Anwendungen), über das die Nutzung von Ressourcen des Smartphones geregelt werden, die Rechte möglichst restriktiv vergeben?	Ja	teilweise	Nein	
	Werden die Rechte der Anwendungen zentral vergeben?	Ja	teilweise	Nein	
	Wenn nein: Sind die Benutzer darauf hingewiesen worden, dass sie keine Einstellungen eigenständig ändern dürfen?	Ja	teilweise	Nein	
	Sind Cloud-Dienste deaktiviert?	Ja	teilweise	Nein	
	*** Betrieb ***				
	Wissen die Benutzer, welche Applikationen sie nutzen dürfen?	Ja	teilweise	Nein	
	Sind nur freigegeben Anwendungen (Applikationen) installiert?	Ja	teilweise	Nein	
	Stammen alle Anwendungen aus vertrauenswürdigen Quellen?	Ja	teilweise	Nein	
	Wurden die Benutzer von Smartphones auf die Regelungen hingewiesen, die von ihnen einzuhalten sind?	Ja	teilweise	Nein	
	Werden die Benutzer auf deren geeignete Aufbewahrung hingewiesen?	Ja	teilweise	Nein	
	*** Patch-Management ***				
	Ist geregelt, dass Anwendungen auf dem neuesten Stand gehalten sind?	Ja	teilweise	Nein	
	Ist geregelt, wer für das Patch-Management zuständig ist?	Ja	teilweise	Nein	
	Erfolgt das Installieren von Sicherheitsupdates umgehend?	Ja	teilweise	Nein	
	Wird wöchentlich das System auf zur Verfügung stehende Sicherheitsupdates überprüft?	Ja	teilweise	Nein	
	Ist geregelt, wer sich um die Systempflege wann kümmert?	Ja	teilweise	Nein	
	*** Virenschutz ***				
	Ist ein aktueller Virenschutz (Virenscanner mit Echtzeitschutz) installiert? Welcher?	Ja	teilweise	Nein	
	Beinhaltet der Virenschutz auch einen Spam-Filter, um unerwünschte E-Mails und SMS zu blocken?	Ja	teilweise	Nein	

	Kann die Anti-Viren-App auch Webseiten auf Schadsoftware überprüfen, bevor sie im Browser geladen wird?	Ja	teilweise	Nein	
	*** Firewall ***				
	Ist eine Firewall installiert? Enthält die Firewall auch Schnittstellenfilterung (z. B. WLAN, USB, Bluetooth)?	Ja	teilweise	Nein	
	*** bei privater Nutzung von Smartphones im Unternehmen ***				
	Ist geregelt, dass auch auf dem privaten Smartphone immer eine aktuelle Virenschutz-Software mit Firewallfunktion installiert wird?	Ja	teilweise	Nein	
	*** Trennung von privatem und dienstlichem Bereich auf Smartphones, Tablets und PDAs ***				
	Werden auf den mobilen Endgeräten dienstliche und private Daten durch einen geschützten Container oder durch eine Virtualisierungslösung voneinander getrennt?	Ja	teilweise	Nein	
	Wird der Datenschutzbeauftragte in die Umsetzung der Maßnahmen zur Trennung von dienstlichen und privaten Daten einbezogen?	Ja	teilweise	Nein	
	Datenschutz				
	Sind Unternehmensdaten auf dem Gerät gespeichert?	Ja	teilweise	Nein	
	Wenn ja: Sind die sensiblen Daten auf dem Gerät ausreichend verschlüsselt?	Ja	teilweise	Nein	
	Sind Cloud-Dienste deaktiviert?	Ja	teilweise	Nein	
	Datensicherung				
	Werden wichtige Daten auf den Smartphones der Anwender regelmäßig (möglichst zentral) gesichert?	Ja	teilweise	Nein	
	Wer ist dafür verantwortlich?	Ja	teilweise	Nein	
	In welchen Zeitabständen?	Ja	teilweise	Nein	
	*** Sperrung des Smartphones bei Verlust oder Diebstahl ***				
	Ist sichergestellt, das Smartphones nach einem Verlust zeitnah gesperrt werden?	Ja	teilweise	Nein	
	Sind alle notwendigen Informationen für die Sperrung eines Smartphones jederzeit griffbereit?	Ja	teilweise	Nein	
	*** Ausgabe Smartphone ***				
	Werden die Benutzer bei Ausgabe eines Smartphones auf die Regelungen und Sicherheitsmaßnahmen hingewiesen, die von ihm einzuhalten sind?	Ja	teilweise	Nein	
	Werden die Benutzer bei Ausgabe eines Smartphones informiert, wie die Geräte aufzubewahren sind?	Ja	teilweise	Nein	
	Werden die Ausgabe des Smartphones und die Hinweise auf Regelungen und Sicherheitsanweisungen dokumentiert?	Ja	teilweise	Nein	
	*** Sicherheitsempfehlungen für den Nutzer ***				
	Gibt es ein Dokument „Sicherheitsmaßnahmen durch die Benutzer“?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Bemerkung
4.12	**Backup-System (Archivierungssystem)**				
	Erfassung				
	Erfolgt die Synchronisierung der Uhrzeit über einen Zeitserver? (wichtig für Log-Auswertung)	Ja	teilweise	Nein	
	Steht der Zeitserver im internen Netz?	Ja	teilweise	Nein	
	Hersteller und Typ?				
	Welche Firmwareversion ist installiert?				
	Gibt es ein Verfahren zur Datensicherung, Datenwiederherstellung und Archivierung?	Ja	teilweise	Nein	
	Aktualität				
	Ist die Firmware auf aktuellem Stand?	Ja	teilweise	Nein	

Maßnahme	Frage	Umsetzung			Anmerkungen
4.13	**DSL-Router**				
	Erfassung				
	Welches Modell wird verwendet (Hersteller und Typ)?				
	Welche Firmwareversion ist installiert?				
	Sind Fernzugriffe über Portweiterleitung oder VPN eingerichtet?	Ja	teilweise	Nein	
	Wenn ja, welche Portweiterleitung?				
	Wenn ja, welche VPN-Anbindung?				
	Liegen die DSL-Zugangsdaten an einem definierten Platz vor?	Ja	teilweise	Nein	
	**** Wartung***				
	Ist die Firmeware auf aktuellem Stand?	Ja	teilweise	Nein	

	Ist eine aktuelle Konfiguration des DSL-Routers gesichert? Wenn ja, wo (an einem anderen Ort)?	Ja	teilweise	Nein	
	Sind alle Wartungsarbeiten (Konfigurationsänderungen, Firmwareupdates, etc.) im Checkheft eingetragen?	Ja	teilweise	Nein	
	Sicherheitsmaßnahmen für Basisschutz				
	Sind die Standardzugangsdaten verändert (z. B. admin/admin)?	Ja	teilweise	Nein	
	Ist ein Kennwortschutz für die Konfigurationsoberfläche vergeben?	Ja	teilweise	Nein	
	Ist ein (Komplexes) Anmeldekennwort eingerichtet?	Ja	teilweise	Nein	
	Sind WPS und UPnP deaktiviert?	Ja	teilweise	Nein	
	Ist die Fernadministration des DSL-Routers deaktiviert?	Ja	teilweise	Nein	

Bereich 5: Vorfall, Störung/Ausfall und Kontinuität

1. Sicherheitsvorfall

2. Störungen und Ausfälle - Notfallmanagement

3. Änderungen und kontinuierliche Verbesserungen - wiederkehrende Überprüfungen

Maßnahme	Frage	Umsetzung			Anmerkungen
5.1	**Sicherheitsvorfall**				
	IS-Richtlinie zum Umgang mit Sicherheitsvorfällen				
	Ist der Umgang mit Sicherheitsvorfällen in einer IS-Richtlinie festgelegt (geregelt)?	Ja	teilweise	Nein	
	Ist jedem Mitarbeiter diese IS-Richtlinie bekannt und hat er die Kenntnisnahme durch seine Unterschrift dokumentiert?	Ja	teilweise	Nein	
	*** Verfahren ***				
	Weiß jeder Mitarbeiter, wann und an wen ein Sicherheitsvorfall zu melden ist?	Ja	teilweise	Nein	
	Gibt es ein Verfahren, das die Reihenfolge der Reaktionen beim Auftreten eines Sicherheitsvorfalls sicherstellt?	Ja	teilweise	Nein	

5.2	Störungen und Ausfälle - Notfallmanagement				
	IS-Richtlinie zum Umgang mit Störungen und Ausfällen				
	Gibt es eine IS-Richtlinie zum Umgang mit Störungen und Ausfällen?	Ja	teilweise	Nein	
	Verfahren beim Auftreten einer Störung oder eines Ausfalls				
	Gibt es ein Verfahren, das die Reihenfolge der Reaktionen beim Auftreten einer Störung oder eines Ausfalls sicherstellt (z. B. Notfall-Handbuch)?	Ja	teilweise	Nein	
	Gibt es Wiederanlaufpläne?	Ja	teilweise	Nein	

5.3	Änderungen und kontinuierliche Verbesserungen - wiederkehrende Überprüfungen				
	Gibt es eine Auflistung der wiederkehrenden Überprüfungen zur Überprüfung der Aktualität von IS-Richtlinien, Verfahren, Konzepten, Netzübergängen, etc.?	Ja	teilweise	Nein	
	Werden jährlich die Funktionstrennungen überprüft?	Ja	teilweise	Nein	
	Wird jährlich ein Lagebericht für die Geschäftsleitung bzw. falls vorhanden das Informationssicherheitsteam erstellt?	Ja	teilweise	Nein	
	Werden jährlich die Netzübergänge zu weniger oder nicht vertrauenswürdigen Netzwerken überprüft?	Ja	teilweise	Nein	
	Weiterentwicklung Datensicherung: Betrifft „IS-Richtlinie für Datensicherung und Archivierung“ sowie „Verfahren zur Datensicherung, Datenwiederherstellung und Archivierung“. Wird jährlich das Datensicherungskonzept auf Weiterentwicklung überprüft?	Ja	teilweise	Nein	
	Test Wiederherstellung: Wird jährlich das Wiederherstellen eines gesicherten IT-Systems nach dem Zufallsprinzip ausgewählt und in einer Testumgebung wiederhergestellt?	Ja	teilweise	Nein	
	Verfahren: Werden jährlich die Verfahren auf Umsetzung, Angemessenheit und Effektivität überprüft?	Ja	teilweise	Nein	
	optional bei kritischen IT-Ressourcen und Risikoanalysen				

	Werden jährlich die Risikoanalysen und –behandlungen auf Aktualität überprüft und bei Bedarf wiederholt?	Ja	teilweise	Nein
	Erfolgt für kritische IT-Ressourcen eine zusätzliche jährliche Prüfung?	Ja	teilweise	Nein
	Wenn ja: Werden Sicherungs- und Wiederherstellungsverfahren für kritische IT-Systeme an einem kritischen IT-System getestet?	Ja	teilweise	Nein
	Wenn ja: Werden alle Zugänge zu kritischen IT-Systemen, sowie sämtliche Zugriffsrechte auf kritische Informationen jährlich erfasst und daraufhin überprüft, ob sie gemäß definierter Verfahren für kritische Verfahren angelegt wurden und benötigt werden?	Ja	teilweise	Nein