

Der IT-Sicherheitscheck!

•O• SECUREPOINT
SECURITY SOLUTIONS



Was tun und Wie es geht!? 15 Minuten für Ihre Sicherheit!

„Bei uns ist noch nie irgendetwas passiert!“

„Datenschutzbeauftragter? Den brauche ich erst ab 10 Mitarbeiter!“

„Bei mir gibt's nichts Interessantes zu holen? Unsere Daten kann niemand gebrauchen!“

„Ich vertraue dem jetzigen Zustand! Bei uns ist alles sicher!“

„Was soll schon passieren!?“

„Ich kenne unsere Mitarbeiter! Wozu kontrollieren, das macht doch nur Arbeit!“

„Ich kenne die Schwachstellen in unserer Firma! Die sind aber nicht so wichtig!“

Dies ist nur ein ganz kleiner Ausschnitt von Aussagen, die in vielen Beratungen vorkommen. Wahrscheinlich würde niemand diese Sätze ernst nehmen, wenn es um den Einsatz einer Kranken- oder Unfallversicherung gehen würde. Und doch wird aus Unkenntnis von Geschäftsführern und IT-Verantwortlichen sehr oft leichtfertig mit dem Thema IT-Sicherheit umgegangen. Und oft mit schwersten Folgen!

Natürlich ist IT-Sicherheit ein komplexes Thema. Das BSI-Grundschutzhandbuch mit über 3000 Seiten macht es den Unternehmen nicht gerade einfach. Wir haben deshalb besonders wichtige Bereiche zusammengefasst, um in 15 Minuten einen guten Überblick über den Zustand eines Unternehmens zu erlangen. Nehmen Sie sich diese Zeit! Sie ist es wert!

Der Sicherheitscheck für:

Kunde

Telefon

Firma

Straße

PLZ/Ort

Ihr Systemhaus und Fachhandelspartner:



Wussten Sie...



... dass Sie gegenüber Dritten mit Bußgeldern bis zu 250.000 Euro haften und das sogar trotz GmbH-Firmierung mit Ihrem Privatvermögen! Zusätzlich können weitere Schadenersatzforderungen auf Sie zukommen!

... dass ein Datenschutzbeauftragter schon unter 10 Angestellten Pflicht für Sie ist, wenn Sie personenbezogene Daten elektronisch verarbeiten!

... dass es Haftstrafen und Bußgelder für die Verbreitung von oder Zugang zu illegalen Daten (Kinderpornografie, Rassismus...) gibt.

... dass Sie Schadenersatz für Bereitstellung und Verbreitung illegaler Raubkopien (Musik, Software...) leisten müssen.

... dass es bald Pflicht ist, 6 Monate Verbindungsdaten zu speichern.

... dass Sie auch dann haften, wenn:

Wenn Sie jemanden (auch unbewusst/unbeabsichtigt) Schaden zufügen:

- Bundesdatenschutzgesetz (BDSG), u. a. §4f, §7, §9, §43,
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG),
- Aktiengesetz (AktG),
- Steuerberatungsgesetz (StBerG),
- Wirtschaftsprüferordnung (WiPrO)

Laut Bundesdatenschutzgesetz (BDSG) muss jede Firma, auch wenn sie nur aus einer Person besteht (z. B. ein Arzt, Handwerker, Hotelier, Steuerberater...) einen Datenschutzbeauftragten haben, wenn personenbezogene Daten am Computer bearbeitet werden.

Wenn Ihre Computer von Fremden mittels Trojaner oder internen Mitarbeitern benutzt werden, müssen Sie mit Haftstrafen und weiteren Folgen rechnen: Strafgesetzbuch (StGB) §184b und Jugendschutzgesetze.

Ein Verstoß gegen das Urheberrecht kann sehr teure Folgen haben. Wenn Auszubildende oder Angestellte – auch nur versehentlich und ohne Ihre Kenntnis – Musikdateien, Filme oder Software aus dem Internet laden, können erhebliche Forderungen auf Sie zukommen.

Bundeskriminalamtgesetz (BKAG). Dies betrifft vor allen Dingen alle Provider und Betreiber von offenen WLANs (Hotels, Gaststätten...)

- kein Mitwissen Ihrerseits vorliegt,
- Mitarbeiter fahrlässig handelten oder einfach etwas ausprobieren wollten,
- Dritte Ihre EDV mittels Trojaner/Bots ohne Ihre Zustimmung benutzen,
- Sie nicht Ihrer Nachweispflicht nachgekommen sind,
- Sie keinen verantwortlichen **Datenschutzbeauftragten** schriftlich bestimmt haben
- und Sie keine geeigneten technischen Maßnahmen durchführen!



Analyse der IT-Sicherheit!

1 Strategische Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Hat die Geschäftsführung die IT-Sicherheitsziele formuliert und sich zu ihrer Verantwortung für die IT-Sicherheit bekannt? Dazu zählen:

- Besteht eine aktuelle, fortlaufende Dokumentation über die wichtigen Anwendungen und IT-Systeme, deren Schutzbedarf und Risiko-Einschätzung? ja nein
- Gibt es ein dokumentiertes IT-Sicherheitskonzept, bestehend aus einem Handlungsplan, der Sicherheitsziele definiert, priorisiert und die Umsetzung der Sicherheitsmaßnahmen regelt? ja nein
- Gibt es Checklisten dafür, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Passwörter, Unterweisungen, Arbeitsanweisungen)? ja nein
- Sind für alle IT-Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt? Gibt es Vertretungsregelungen? ja nein
- Sind die bestehenden Richtlinien und Zuständigkeiten allen Mitarbeitern bekannt und können diese jederzeit auf diese Dokumentation zugreifen? ja nein
- Ist ein IT-Sicherheitsbeauftragter/-Datenschutzbeauftragter¹ schriftlich ernannt worden? Ist dieser qualifiziert? ja nein
- Gibt es einen schriftlichen Risiko-Plan, um auch bei EDV-Ausfällen arbeiten zu können? ja nein
- Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen² regelmäßig überprüft? ja nein
- Sind und werden gesetzliche und/oder vertragsrechtliche Gesichtspunkte in der unternehmensweiten IT-Sicherheit berücksichtigt? ja nein
- Werden IT-Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffung von IT-Systemen und Anwendungen)? ja nein
- Sind die eingesetzten Security-Produkte zukunftssicher, geprüft³ und erlauben diese, dass der Netzwerkverkehr überwacht, gefiltert, protokolliert und diese Daten zur Kontrolle archiviert werden können? ja nein
- Werden vertrauliche Informationen und Datenträger sorgfältig aufbewahrt/archiviert? ja nein
- Werden vertrauliche Informationen vor Wartungs- und Reparaturarbeiten von Datenträgern gelöscht/gesichert? ja nein
- Werden Mitarbeiter regelmäßig in sicherheitsrelevanten Themen geschult? ja nein
- Gibt es Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter? ja nein
- Werden bestehende Sicherheitsvorgaben kontrolliert und Verstöße geahndet? ja nein

¹ Achtung: auch bei Unternehmen <10 Mitarbeiter bei Verarbeitung personenbezogener Daten

² Wie hoch ist die Häufigkeit?

³ Speziell Ärzte und Kliniken sollten auf KV-SafeNet achten!

Anzahl:

ja nein



2 Operative Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Rechte der Anwender:

- Sind den Systembenutzern Rollen und Profile zugeordnet worden und ist geregelt, auf welche Datenbestände Anwender zugreifen dürfen?
- Gibt es ein Konzept, welche Daten nach innen und außen angeboten werden?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Warten von IT-Systemen: Umgang mit Updates:

- Gibt es einen Verantwortlichen, der sich über Sicherheitseigenschaften der Systeme und relevanter Sicherheitsupdates informiert?
- Werden Sicherheits-Updates immer eingespielt?
- Gibt es ein Testkonzept für Systemänderungen?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Passwörter und Verschlüsselung:

- Bieten Programme und Anwendungen Sicherheitsmechanismen (Passwortschutz/Verschlüsselung)? Sind die Sicherheitsmechanismen aktiviert?
- Wurden voreingestellte/leere Passwörter geändert?
- Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
- Werden Arbeitsplatzrechner bei Verlassen mit Bildschirmschoner und Kennwort gesichert?
- Werden vertrauliche Daten und gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen geschützt?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Notfallvorsorge:

- Sind die wichtigsten Passwörter für Notfälle hinterlegt?
- Gibt es einen Notfallplan mit Anweisungen und Kontaktadressen?
- Werden relevante Notfallsituationen behandelt?
- Kennt jeder Mitarbeiter den Notfallplan. Ist er zugänglich?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Datensicherung:

- Gibt es eine Backup-Strategie und ist festgelegt, welche Daten wie lange und wo gesichert werden?
- Bezieht die Sicherung auch tragbare Computer und nicht vernetzte Systeme mit ein?
- Sind die Sicherungs- und Rücksicherungsverfahren dokumentiert?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Infrastruktursicherheit:

- Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überhitzung, Wasserschäden, Überspannung und Stromausfall?
- Ist der Zutritt zu IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden?
- Besteht ein ausreichender Schutz vor Einbrechern?
- Ist der Bestand an Hard- und Software in einer Inventarliste erfasst?

<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>

Anzahl:

<input type="checkbox"/>	<input type="checkbox"/>
--------------------------	--------------------------



Wo stehen Sie?

Auswertung Ihres Unternehmens:

Diese Checkliste soll Sie sensibilisieren. Sie zeigt Ihnen wesentliche Lücken in der IT-Sicherheit im Unternehmen auf und hilft Ihnen eine angemessene Lösung zu finden.

Grundsätzlich sollten Sie alle Fragen in allen Bereichen der Checkliste mit „Ja“ beantworten, nur dann können Sie sicher sein, dass Sie auf dem richtigen Weg sind!

Diese strukturierte Vorgehensweise und das Feststellen des Bedarfs in IT-Sicherheit soll Ihnen einerseits die Gewissheit geben das Optimale zu tun, aber auch klar aufzeigen:

„Wo sind die Schwächen, was ist wichtig, was muss getan werden und steht alles in einem vernünftigen Kosten-/Nutzenverhältnis!“

1 Strategische Sicherheit

- **0 bis 8 Fragen beantwortet:**
Sie sollten sich äußerst dringend zum Thema IT-Sicherheit beraten lassen!
- **10 bis 13 Fragen beantwortet:**
Gut, dass Sie etwas tun! Jedoch sollten Sie schnell die offenen Fragen abarbeiten.
- **14 bis 16 Fragen beantwortet:**
Gratuliere, Sie haben es fast geschafft ein Vorzeige-Unternehmen im Bereich IT-Security zu sein! Aber haben Sie das alles auch operativ umgesetzt?

2 Operative Sicherheit

- **0 bis 10 Fragen beantwortet:**
Leider haben Sie kaum etwas in der IT-Sicherheit umgesetzt. Sehr große Schwierigkeiten können auf Sie zukommen!
- **11 bis 17 Fragen beantwortet:**
Sie haben schon einige richtige Schritte im Bereich IT-Sicherheit getan. Sie müssen jedoch noch viel mehr tun.
- **18 bis 21 Fragen beantwortet:**
Gratuliere, wenn Sie für die strategische Sicherheit im Unternehmen genauso viel getan haben wie im operativen Bereich, dann sind Sie ein Gewinner.



■ ■ ■ ■ ■ Projekt-Daten, die benötigt werden!

Infrastruktur / Projektcheckliste

Checkliste für Projekt-Dokumentation und Appliance-Auswahl:

Weitere Informationen:

1 Internet-Anbindungen:

- Provider¹: _____

- Multi Path Routing² benötigt: _____
- QoS/Bandbreitenbindung für Dienste/Ports (VPN, Mail)?
Beschreibung: _____

- Anbindung:
 Standleitung ADSL SDSL
 mit DynDNS
- Gebuchte Bandbreite:
 2 MBit³ 4 MBit 16 MBit >16 MBit: _____
- Gesamt-Daten-Traffic am Tag⁴: _____
- Vorhandene Kommunikationshardware
 DSL-Modem Router: _____

¹ Providerdaten für Authentisierung vorhanden?

² Unterstützung mehrerer DSL-Leitungen an einer Appliance für Redundanz/Load-Balancing und größere Bandbreiten

³ bei kleinerer Userzahl ausreichend

⁴ Wichtig für Appliance-Auswahl

2 VPN-/Filial-Anbindungen:

- Gegenstelle(n) mit
 DSL⁵, Anzahl: _____
 Bandbreiten⁶: _____
- Hardware der Gegenstelle
 Router (Modell/Version), Anzahl: _____
 Securepoint (Modell/Version), Anzahl: _____
 Sonstige (Modell/Version), Anzahl: _____

- VPN-Clients
 Anzahl VPN-Benutzer: _____
 XP-/Vista-VPN⁷ (L2TP) Greenbow
 OpenVPN IPSec
 PPTP⁸ Sonstige: _____
- Art der Authentisierung
 PSK X.509 Sonstige: _____
 Anzahl der VPN-Anwender⁹: _____

⁵ DSL384 eventuell ungeeignet

⁶ Bandbreite vielleicht nicht groß genug

⁷ für Standardumgebung ausreichend

⁸ Sollte nicht mehr eingesetzt werden!

⁹ für Standardumgebung ausreichend

3 Administration der Security-Umgebung/-Appliance:

- Administrator des Unternehmens verfügbar/vor Ort¹⁰
- Windows-PC verfügbar¹¹ als Emulation auf MAC/Linux¹¹

¹⁰ ggf. Technical Assistance benötigt

¹¹ Für Securepoint Security Manager notwendig!

Weitere Informationen:

4 Serverumgebung:

- Windows-Server, Anzahl/OS-Version: _____
- Linux-Server, Anzahl/OS-Version: _____
- IBM i-Series, Anzahl/OS-Version¹²: _____
- andere Großrechner, Anzahl, OS-Version¹²: _____
- Anwendungen¹²: _____

¹² Protokolle notieren!

5 Netzaufteilung:

- Anzahl interne Netze¹³: _____
- IP-Netzkreise

<input type="checkbox"/> von _____ bis _____
<input type="checkbox"/> von _____ bis _____
<input type="checkbox"/> von _____ bis _____
<input type="checkbox"/> von _____ bis _____
<input type="checkbox"/> von _____ bis _____

¹³ auf die Anzahl der verfügbaren Interfaces (DMZs) der Security-Appliance achten!

6 Mail:

- Mail-Protokoll:

<input type="checkbox"/> POP3	<input type="checkbox"/> SMTP-Gateway
<input type="checkbox"/> Virenschanning	<input type="checkbox"/> Nutzung eines Spamfilters?
	<input type="checkbox"/> Mail-Gateway vom Internet nutzbar?
- Mail-Aufkommen¹⁴:
 - Anzahl Mail am Tag (incomming/outgoing), ca.: _____
 - Einkommende Mails pro Tag (inkl. Spam-Mails), ca.: _____
 - Mail-Server und -Typ: _____

¹⁴ ggf. Anpassung der Hardware-Performance

7 Interne Nutzer:

- Anzahl Mitarbeiter¹⁵: _____
- Authentifizierung an der Security-Appliance:

<input type="checkbox"/> Lokale DB ¹⁶	<input type="checkbox"/> Radius	<input type="checkbox"/> Active Directory (AD)/LDAP
--	---------------------------------	---

¹⁵ Bei sehr hohem Daten-/Mail-Traffic sollten größere Appliances gewählt werden

¹⁶ für kleine Netze ausreichend

8 Logging/Reporting:

- Log-Server¹⁷ erwünscht: ja nein

¹⁷ Log-Server ist schon für alle Securepoint Appliances kostenlos vorhanden.

9 Hochverfügbarkeit:

- Hochverfügbarkeit erwünscht: ja nein
 - Anzahl Spare-Lizenzen¹⁸: _____

¹⁸ parallel laufende Security-Appliances, die bei Ausfall der Master-Appliance die Arbeit übernehmen

10 Wartung:

- Subscription (obligatorisch für ein Jahr):

<input type="checkbox"/> 1 Jahr	<input type="checkbox"/> 2 Jahr ¹⁹	<input type="checkbox"/> 3 Jahr ¹⁹
---------------------------------	---	---
- Technical Assistance

<input type="checkbox"/> 1 Jahr	<input type="checkbox"/> 2 Jahr ¹⁹	<input type="checkbox"/> 3 Jahr ¹⁹
---------------------------------	---	---

¹⁹ optional mit Rabatten

11 Leasing:

- Leasing²⁰ erwünscht: ja nein

²⁰ Geringe monatliche Kosten, alle Kosten von der Hardware bis zu Wartungsarbeiten können geleast werden!

Jede Menge Fragen zur Sicherheit...



**... für die Ihr Systemhaus
kompetente Antworten hat!**

Ihr Fachhandelspartner:

**Jede Menge IT-Security-Fragen,
die Antworten verlangen:**

- **Wo sind meine Schwachstellen? Muss ich überhaupt etwas tun?**
- **Was habe ich nicht bedacht?**
- **Wie kann ich mich absichern?**
- **Was weiß ich eigentlich alles über die IT im Unternehmen?**
- **Welche Maßnahmen sind überhaupt sinnvoll?**
- **Welche Risiken/Konsequenzen gibt es für mich. Wo sind speziell meine Schwachstellen?**
- **Mit welchen Gesetzen kann ich in Konflikt kommen?**
- **Wie gehe ich mit den EDV-Systemen und Daten im Unternehmen um?**
- **Wie kann ich schnell meine Situation verbessern?**

**Ihr kompetentes Systemhaus
findet die qualifizierten Antworten,
um Sicherheit zu schaffen!**