

Der IT-Sicherheits-Check! für Ihr Unternehmen

•●• SECUREPOINT
SECURITY SOLUTIONS



Was tun und wie es funktioniert: 15 Minuten für Ihre Sicherheit!

IT-Sicherheit ist ein komplexes Thema für Unternehmen – heute mehr denn je!

In 15 Minuten gibt Ihnen diese Broschüre einen Überblick über den Sicherheitszustand Ihres Unternehmens und fasst die aktuell wichtigen Themen im Bereich IT-Security klar und verständlich zusammen. Gleichzeitig erhalten Sie einen Projektleitfaden, um Ihr Unternehmen optimal zu schützen und rechtssicher aufzustellen.

SecurITy
made
in
Germany



Wussten Sie...



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

... dass ein Datenschutzbeauftragter schon bei unter 20 Angestellten Pflicht für Sie ist, wenn Sie personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeiten!

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

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

... dass es Pflicht wird, Verbindungsdaten zu speichern, denn EU-Gesetze zur Vorratsdatenspeicherung werden in Kürze in Deutschland umgesetzt.

... dass personenbezogene Log-Daten nicht so einfach zum Nachweis von Taten verwendet werden dürfen:

... dass Sie auch dann haften, wenn:

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

- Bundesdatenschutzgesetz (BDSG)
- Telekommunikationsgesetz (TKG)
- GmbH-Gesetz (GmbHG),
- Aktiengesetz (AktG),
- Steuerberatungsgesetz (StBerG),
- Wirtschaftsprüferordnung (WiPrO)

Laut Bundesdatenschutzgesetz (BDSG) muss jede Firma, auch unter 20 Angestellten (z. B. Ärzte, Steuerberater, Rechtsanwälte...) einen Datenschutzbeauftragten bestellen, wenn personenbezogene Daten geschäftsmäßig elektronisch zur Übermittlung verarbeitet werden.

Wenn Ihre Computer von Fremden mittels Trojaner/Bots benutzt werden, können Sie mit Haftstrafen und weiteren Folgen rechnen: Strafgesetzbuch (StGB) §184b und Jugendschutzgesetze.

Ein Verstoß gegen das Urheberrecht kann teuer werden. Wenn Azubis oder Angestellte – auch versehentlich und ohne Ihre Kenntnis – illegal Musikdateien, Filme, Software etc. aus dem Internet laden, können Sie haftbar gemacht werden.

EU-Gesetze zur Vorratsdatenspeicherung: Dies betrifft vor allen Dingen alle Provider und Betreiber von Kunden-WLANs (Flughäfen, Hotels, Gaststätten...)

Betriebsverfassungsgesetz, Arbeitsrecht und Vier-Augen-Prinzip: Nur ein Datenschutzbeauftragter und Administrator dürfen gemeinsam auf personenbezogene Log-Daten zugreifen. Die Daten müssen verschlüsselt sein oder es muss eine unterschriebene Betriebsvereinbarung vorliegen.

- 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 bestellt haben
- und Sie keine geeigneten technischen IT-Schutzmaßnahmen 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?
- Gibt es ein dokumentiertes IT-Sicherheitskonzept, bestehend aus einem Handlungsplan, der Sicherheitsziele definiert, priorisiert und die Umsetzung der Sicherheitsmaßnahmen regelt?
- Gibt es Checklisten dafür, was beim Eintritt neuer Mitarbeiter und beim Austritt von Mitarbeitern zu beachten ist (Berechtigungen, Schlüssel, Passwörter, Unterweisungen, Arbeitsanweisungen)?

☐ ☐

Mindestens einmal jährlich sollten alle IT-Schutzmaßnahmen definiert und überprüft werden. Neben der allgemeinen Sicherheit für Ihr Unternehmen, wird das bzgl. Basel II und III als Softfact auch Ihre Unternehmensbilanz bei der Bank verbessern. Weisen Sie die Bank im Bilanzgespräch darauf hin!

- Werden Mitarbeiter regelmäßig zu sicherheitsrelevanten Themen geschult?

☐ ☐

Ihre Mitarbeiter müssen wissen, was IT-Security bedeutet und was Sie im Unternehmen durchsetzen wollen.

- Gibt es personelle und technische Maßnahmen zur Erhöhung des Sicherheitsbewusstseins der Mitarbeiter?

☐ ☐

- Sind für alle IT-Sicherheitsmaßnahmen Zuständigkeiten und Verantwortlichkeiten festgelegt? Vertretungsregelungen?

☐ ☐

- Sind die bestehenden Richtlinien und Zuständigkeiten allen Mitarbeitern bekannt und können diese jederzeit auf diese Dokumentation zugreifen?

☐ ☐

- Ist ein IT-Sicherheitsbeauftragter/Datenschutzbeauftragter¹ schriftlich benannt worden und ist dieser qualifiziert?

☐ ☐

Achtung: Auch bei Unternehmen <20 Mitarbeiter ist bei der elektronische Verarbeitung personenbezogener Daten zum Zweck der Übermittlung ein Datenschutzbeauftragter notwendig.

- Gibt es einen schriftlichen Risiko-Plan, um auch bei EDV-Ausfällen arbeiten zu können?

☐ ☐

- Wird die Wirksamkeit von IT-Sicherheitsmaßnahmen² regelmäßig überprüft?

☐ ☐

- Sind und werden gesetzliche und/oder vertragsrechtliche Gesichtspunkte in der unternehmensweiten IT-Sicherheit berücksichtigt?

☐ ☐

- Werden IT-Sicherheitserfordernisse bei allen Projekten frühzeitig berücksichtigt (z. B. bei Planung eines neuen Netzes, Neuanschaffung von IT-Systemen und Anwendungen)?

☐ ☐

Speziell Ärzte und Kliniken sollten auf KV-SafeNet achten!

- Ermöglichen die eingesetzten Security-Produkte, dass der Netzwerkverkehr überwacht, gefiltert, protokolliert und diese Daten archiviert werden können?

☐ ☐

Log-Daten zum späteren Nachweis sind verschlüsselt zu erfassen und dürfen nur durch einen Datenschutzbeauftragten und Administrator gemeinsam angesehen werden. So können die Daten bei Rechtsverstößen (Arbeitsrecht, Betriebsverfassungsgesetz...) gerichtlich verwendet werden.

- Werden Log-Daten für einen späteren Nachweis bei Vorfällen rechtskonform und über die Dauer von 10 Jahren gesichert?

☐ ☐

- Werden vertrauliche Informationen vor Wartungs- und Reparaturarbeiten von Datenträgern gelöscht/gesichert?

☐ ☐

- Wurde eine Betriebsvereinbarung unterzeichnet, die regelt, was im Unternehmen erlaubt ist und was nicht, z. B.: Darf auf Log-Daten zugegriffen werden, darf ein Mitarbeiter Downloads durchführen, werden illegale Webseiten gesperrt, ist die Privat-Nutzung von Firmen-E-Mails erlaubt oder nicht und wenn ja, darf auf diese zugegriffen werden etc.?

☐ ☐

- Werden und wie werden Verstöße gegen die IT-Security-Richtlinien in Ihrem Unternehmen geahndet?

☐ ☐

Was sind die Folgen für Mitarbeiter: Abmahnungen etc.

Anzahl:



2 Operative Sicherheit

Bitte beantworten Sie nun die folgenden Fragen:

Antwort:

ja nein

Notizen

Client- und Netzwerkschutz:

- Ist auf Clients (Rechner, Server, mobile Geräte etc.) ein aktuelles Schutz-Programm (Firewall, AV-Programm) installiert?
- Ist zum Gesamtschutz für das Netzwerk ein UTM-System bestehend aus Firewall, AV, VPN-Server, Spam-Filter, Web-Filter, Intrusion Detection, Log-Server etc. installiert?
- Werden regelmässige monatliche Reports gemacht, aus der die Unternehmensleitung ersieht: Was passiert im Netzwerk, wer macht was und wo sind Schwachstellen?
- Werden bei einer Standortvernetzung bzw. Homearbeitsplätzen Daten hochverschlüsselt übermittelt (VPN)?

Rechte der Anwender, Umgang mit Passwörtern:

- Sind den IT-Benutzern Rollen und Profile zugeordnet worden?
- Sind alle Mitarbeiter in der Wahl sicherer Passwörter geschult?
- Werden Computer beim Verlassen mit Passwörtern gesichert?
- Wird überprüft, ob Passwörter irgendwo öffentlich notiert sind?
- Wurden voreingestellte oder leere Passwörter geändert?

Notfallvorsorge:

- Gibt es einen Verantwortlichen, der sich über Sicherheits-eigenschaften der Systeme und relevante Sicherheits-Updates informiert und die IT-Systeme schnell aktualisiert?
- Sind die wichtigsten Passwörter für Notfälle sicher hinterlegt?
- Gibt es einen Notfallplan mit Anweisungen/Kontaktadressen?
- Kennt jeder Mitarbeiter den Notfallplan und ist er zugänglich?

Reports, Datenschutz/Verschlüsselung:

- Gibt es ein Konzept, das beschreibt, welche Daten nach innen und nach außen (zum Internet) angeboten werden?
- Ist geregelt, auf welche Daten Anwender zugreifen dürfen?
- Wird geloggt/reportet: Wer hat was im Netzwerk gemacht und wer ist verantwortlich?
- Werden gesetzliche Aufbewahrungspflichten berücksichtigt?
- Werden personenbezogene Daten sicher verarbeitet?
- Sind die Sicherheitsmechanismen auch aktiviert?
- Werden vertrauliche Daten und gefährdete Systeme wie Notebooks ausreichend durch Verschlüsselung oder andere Maßnahmen – z. B. bei Verlust/Diebstahl – geschützt?

Wartung von IT-Systemen, 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-/Rücksicherungsverfahren dokumentiert?
- Gibt es ein Testkonzept bei Systemänderungen?

Infrastruktursicherheit:

- Besteht ein angemessener Schutz der IT-Systeme gegen Feuer, Überspannung, Wasserschäden und Stromausfall?
- Ist der Zutritt zu IT-Systemen und Räumen geregelt? Müssen Besucher, Handwerker, Servicekräfte etc. begleitet bzw. beaufsichtigt werden? Ist ein Einbruchschutz vorhanden?

Anzahl:

Beachten Sie, viele Netzwerk-Systeme (Kopierer/Drucker, Fax, Switch, spezielle Server, die Netzwerkkommunikation etc.) können nicht direkt geschützt werden, das geht nur mittels einer UTM. Außerdem verfügen Sie damit gemeinsam mit dem Clientschutz über ein zweistufiges Sicherheitssystem.

Z. B. Passwörter auf Haftnotizen!
Oftmals wird vergessen, die Passwörter der Werkseinstellung von IT-Systemen zu verändern!

Was tun bei Notfällen!
Betriebsunterbrechung vermeiden, denn das kostet Geld!

Monatliche UTM-Reports zeigen der Firmenleitung auf, was im Netzwerk los ist und wie Probleme gelöst werden können: Mitarbeiter surfen zu viel im Internet, wer macht genau was und welche Kosten verursacht es. Es gibt immer mehr Vorfälle, in denen Know-How, Vertriebsdaten, personenbezogene Daten etc. aus Firmen entwendet werden bzw. diese damit erpresst werden. Eine Vielzahl von Daten unterliegen gesetzlichen Archivierungsrichtlinien, z. B. kaufmännische Daten (Rechnungen etc.) müssen 10 Jahre aufbewahrt werden, Log-Daten unterliegen arbeitsrechtlichen bzw. dem Betriebsverfassungsschutz-Gesetzen. Hier kann Ihnen das Securepoint UMA (Unified Mail Archive) helfen.



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 10 Fragen beantwortet:**
Sie sollten sich äußerst dringend zum Thema IT-Sicherheit beraten lassen!
- **11 bis 14 Fragen beantwortet:**
Gut, dass Sie etwas tun! Jedoch sollten Sie schnell die offenen Fragen abarbeiten.
- **15 bis 17 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 14 Fragen beantwortet:**
Achtung: Sie haben zu wenig in der IT-Sicherheit umgesetzt. Sehr große Schwierigkeiten könnten auf Sie zukommen!
- **15 bis 22 Fragen beantwortet:**
Sie haben schon einige richtige Schritte im Bereich IT-Sicherheit getan. Sie müssen jedoch noch viel mehr tun.
- **23 bis 26 Fragen beantwortet:**
Gratuliere, wenn Sie für die strategische Sicherheit im Unternehmen genauso viel getan haben wie im operativen Bereich, dann sind Sie ein Gewinner!



Benötigen Sie Hilfe für Ihr Netzwerk oder haben Sie weitere Fragen zur IT-Sicherheit?



Wir helfen Ihnen gerne! Ihr Systemhaus!

Ihr Systemhaus-Partner:



Hübner Computer Systeme GmbH

IT-Lösungen mit Kompetenz

Bichlmannstr. 11 - 84174 Eching bei Landshut
08709 9233-0 / www.hcs-huebner.de

••• SECUREPOINT
SECURITY SOLUTIONS

Securepoint GmbH
Salzstraße 1
21335 Lüneburg
Germany

fon: ++49 (0) 41 31 / 24 01-0
fax: ++49 (0) 41 31 / 24 01-50

mail: info@securepoint.de
web: www.securepoint.de