IT-SICHERHEIT FÜR LEITENDE IN KLEINEN UND MITTLEREN UNTERNEHMEN

LERNEINHEIT 7

Berufsschüler BOTTOM-UP! für IT-Sicherheit

DIE THEMEN:

1. GESETZLICHE BESTIMMUNGEN

> Was ist Informationssicherheit
> persönliche Haftung von Geschäftsführern
> Datenschutz-Grundverordnung und IT-Sicherheitsgesetz

2. ORGANISATORISCHE PRÄVENTION

> Technisch-organisatorische Maßnahmen
> Fokus Mitarbeiter
> IT-Sicherheitsbeauftragte*r
> Sicherheitsrichtlinien

3. SCHUTZ VOR WIRTSCHAFTSSPIONAGE

> Angriffe von innen und außen
> Zusammenarbeit mit Externen

1. GESETZLICHE BESTIMMUNGEN

WAS IST INFORMATIONSSICHERHEIT?

	Vertraulichkeit	Verfügbarkeit	Integrität	(Authentizität)
Bedeutung	Gespeicherte Information muss vor unbefugtem Zugriff geschützt werden	Notwendige Informationen und Technik müssen immer genau dann nutzbar bzw. einsatzbereit sein, wenn sie gebraucht werden	Gespeicherte Informationen dürfen nicht verfälscht werden	Informationen stammen tatsächlich vom angegebenen Absender (wichtig beim elektronischen Datenaustausch)
Hintergrund	Personenbezogene Informationen (z.B. Kundenkontaktdaten) dürfen nicht in fremde Hände gelangen	Alle zum Übertragen, Lesen und Bearbeiten der Informationen erforderlichen Systeme – zum Beispiel Computer, Netzwerk und Anwendersoftware – müssen funktionieren	Es besteht die Gefahr, dass manipulierte Hard- oder Software unerwünschte Funktionen ausführt und dadurch Daten verfälscht oder falsche Ergebnisse erzeugt	Gefahr, dass Daten nicht nur von der als Absender benannten Stelle kommen, sondern auch von Personen unbekannter Identität, die sich als der erwartete Absender ausgeben

1. GESETZLICHE BESTIMMUNGEN

PERSÖNLICHE HAFTUNG VON GESCHÄFTSFÜHRERN

Mangelnde interne IT-Sicherheit führt anderen Unternehmen **Schäden** zu

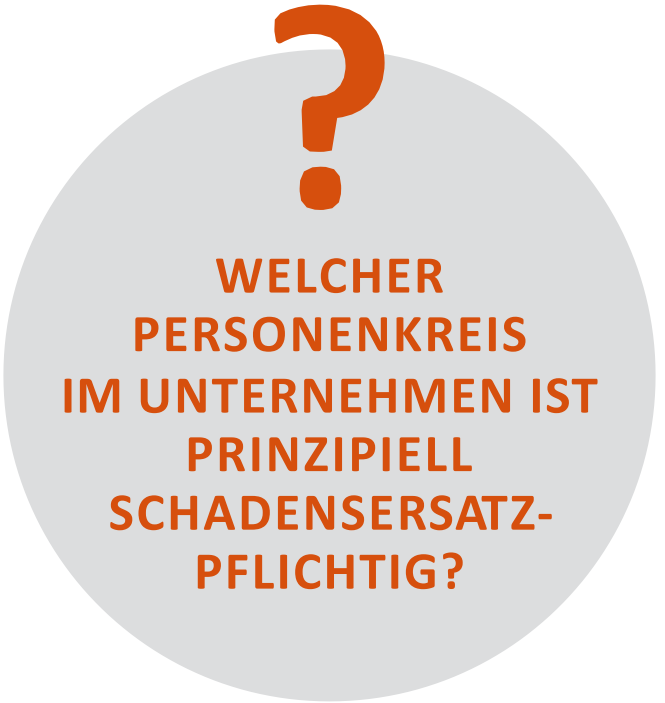
Beispiel: Produktionsausfall

Verschuldensunabhängige (!) Verstöße gegen den Datenschutz gemäß **Bundesdatenschutzgesetz** und daraus entstandene Schäden

Beispiel: die unzulässige bzw. falsche Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten

1. GESETZLICHE BESTIMMUNGEN

PERSÖNLICHE HAFTUNG VON GESCHÄFTSFÜHRERN



Das **Haftungsrisiko** betrifft grundsätzlich nicht nur den unmittelbaren **IT-Verantwortlichen**, sondern auch die **Geschäftsführer**

Ausnahme laut BGH:

GmbH-Geschäftsführer und -Eigentümer
Hier gilt das Prinzip der schadens-ersatzrechtlichen Innenhaftung

1. GESETZLICHE BESTIMMUNGEN

PERSÖNLICHE HAFTUNG VON GESCHÄFTSFÜHRERN

Schutz vor Schadensersatzansprüchen:

- ✓ Nutzung nicht-lizensierter Software konsequent untersagen
- ✓ Risiko des Eindringens von Schadsoftware minimieren
- ✓ Abschluss einer speziellen IT-Haftpflichtversicherung

Datenschutzbeauftragte:

- ✓ vorgeschriebenen, sobald personenbezogene Daten von mehr als neun Personen verarbeitet werden
- ✓ weisungsfrei und unabhängig
- ✓ Fachkunde und Zuverlässigkeit

1. GESETZLICHE BESTIMMUNGEN

DATENSCHUTZ – GRUNDVERORDNUNG

2018 EU– DS-GVO EUROPAWEIT BINDEND AB MAI 2018!

> definiert konkrete Rechte für Unternehmen, den einzelnen Bürger sowie Arbeitnehmer und Arbeitgeber

> betrifft ganz oder teilweise (nicht-)automatisierte Verarbeitung personenbezogener Daten

> enthält Vorgaben für den Transfer von personenbezogenen Daten in Staaten außerhalb der EU

> Marktortprinzip verpflichtet auch Unternehmen außerhalb der EU zur Einhaltung der DS-GVO. Wenn sich deren Angebot an den europäischen Markt richtet.

1. GESETZLICHE BESTIMMUNGEN

IT – SICHERHEITSGESETZ

GESETZ ZUR ERHÖHUNG DER SICHERHEIT INFORMATIONSTECHNISCHER SYSTEME (IT-SICHERHEITSGESETZ)

> betrifft alle Betreiber kommerzieller Internetseiten

> stellt bestimmte Mindestanforderungen an die technischen und organisatorischen Maßnahmen, die Unternehmen zum Schutz ihrer Kundendaten und ihrer IT-Systeme zu erfüllen haben

> enthält spezielle Verordnungen (KRITIS) für Betreiber kritischer Infrastrukturen (wie etwa Strom- und Wasserversorgungs-unternehmen)

2. ORGANISATORISCHE PRÄVENTION

TECHNISCH – ORGANISATORISCHE MASSNAHMEN

- ✓ Installation und Nutzung separater Schutzsysteme (Firewall und Antivirenprogramm)
- ✓ regelmäßige vollständige Systemscans mit der Antiviren-Software
- ✓ nur als ausreichend sicher geltende Passwörter/Verfahren verwenden
- ✓ Daten/Informationen nur in verschlüsselter Form speichern
- ✓ Dateizugriffs- und -bearbeitungsrechte für jeden einzelnen Mitarbeiter regeln
- ✓ automatische Logins in Systeme vermeiden
- ✓ Regelmäßige Datensicherungen durchführen!

2. ORGANISATORISCHE PRÄVENTION

TECHNISCH – ORGANISATORISCHE MASSNAHMEN

- ✓ Vorschriften zum Umgang mit ausrangierten Datenträgern!
- ✓ Dokumentation der IT-Systemkonfiguration und der verwendeten Sicherheitsmaßnahmen anlegen
- ✓ Dokumentation auf sichere Weise hinterlegen
- ✓ spezielle IT-Haftpflichtversicherung mit ausreichender Versicherungssumme abschließen

2. ORGANISATORISCHE PRÄVENTION

FOKUS MITARBEITER

Maßnahmen zur Sensibilisierung

- ✓ Mitarbeiter*innen müssen regelmäßig zum Thema geschult werden
- ✓ mögliche Folgen und potentielle Risiken aufzeigen
- ✓ Sicherheitsregeln dokumentieren
- ✓ auf einwandfreies und sicheres Verhalten im Unternehmen hinweisen

2. ORGANISATORISCHE PRÄVENTION

INFORMATIONSSICHERHEITSBEAUFTRAGTE*R

Beispielhafte Aufgaben

- ✓ Erstellung, Umsetzung und Kontrolle der Einhaltung der unternehmensspezifischen Sicherheitsrichtlinie
- ✓ Notfallvorsorge betreiben (u. a. Notfallhandbuch erstellen)
- ✓ Analyse und die Nachbearbeitung von Informationssicherheitsvorfällen

UNBEDINGT im Unternehmen benennen
– wie auch Datenschutzbeauftragte*n!

2. ORGANISATORISCHE PRÄVENTION

DATENSCHUTZBEAUFTRAGT*E

Beispielhafte Aufgaben

- ✓ Wirkt auf die Einhaltung der Vorschriften des BDSG hin
- ✓ kontrolliert die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen

UNBEDINGT im Unternehmen benennen
– wie auch Informationssicherheitsbeauftrage*n!

2. ORGANISATORISCHE PRÄVENTION

SICHERHEITSRICHTLINIEN IM UNTERNEHMEN

ZWECK

> Verdeutlichen des hohen Stellenwerts der IT-Sicherheit im und für das Unternehmen

> Unterscheidet sich von der Sicherheitsrichtlinie zur IT-Nutzung

> Wird in der Regel vom IT-Sicherheitsbeauftragten anfertigen

INHALTE

> Benennt nur die grundlegenden Sicherheitsziele

> Enthält organisatorische Informationen

> Gibt allgemeine Rahmen-bedingungen vor

3. SCHUTZ VOR WIRTSCHAFTSSPIONAGE

ANGRIFFE VON INNEN UND AUSSEN

ANGRIFF VON AUSSEN

Mitarbeiter*in besitzt i.d.R. Kenntnis über vorhandene Sicherheitsmaßnahmen

> Sicherung von Räumen und / oder Geräten gegen den Zutritt /Zugriff durch unbefugte Personen

> alle auf elektronischem Wege erfassten Daten nur in verschlüsselter Form abspeichern

Schutz und Erkennung durch Firewall, Antivirensoftware etc. möglich

> Systeme regelmäßig aktualisieren / patchen

ANGRIFF VON INNEN

3. SCHUTZ VOR WIRTSCHAFTSSPIONAGE

ZUSAMMENARBEIT MIT EXTERNEN

WICHTIGE SICHERHEITSHINWEISE:

- Daten nur in verschlüsselter Form versenden
- Beim Upload auf eine Internetseite oder ein Cloud-Laufwerk auf eine gesicherte Verbindung achten (erkennbar an der Adresse „https://...“=)
- Beim Empfang von E-Mails prüfen, ob sie tatsächlich vom behaupteten Absender stammen

Berufsschüler BOTTOM-UP! für IT-Sicherheit

Bottom-Up: Berufsschüler für IT-Sicherheit hat zum Ziel, die Mitarbeiter*innen von morgen bereits während der dualen Ausbildung auf die Herausforderungen des digitalen Arbeitsalltags im Hinblick auf IT-Sicherheit und Schutz von Daten vorzubereiten. Damit leistet Bottom-Up einen wichtigen Beitrag zu mehr IT-Sicherheit in kleinen und mittelständischen Unternehmen. www.dsin-berufsschulen.de

Bottom-Up: Berufsschüler für IT-Sicherheit ist ein Angebot von
Deutschland sicher im Netz e.V.
Albrechtstraße 10 / 10117 Berlin
www.sicher-im-netz.de

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Im Rahmen der Initiative:

IT-Sicherheit IN DER WIRTSCHAFT

Ein Projekt von:

DsiN Deutschland sicher im Netz

Initiative „IT-Sicherheit in der Wirtschaft"
Die Initiative „IT-Sicherheit in der Wirtschaft" des Bundesministeriums für Wirtschaft und Energie will vor allem kleine und mittelständische Unter-nehmen beim sicheren Einsatz von IKT-Sys-temen unterstützen. Gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung soll eine Grundlage dafür geschaffen werden, um die Bewusstseinsbildung in der digitalen Wirtschaft beim Thema IT-Sicherheit im Mittelstand zu stärken. Unternehmen sollen durch konkrete Unterstützungsmaßnahmen dazu befähigt werden, ihre IT-Sicherheit zu verbessern. Weitere Informationen zur Initiative und ihren Angeboten sind unter: www.it-sicherheit-in-der-wirtschaft.de abrufbar.