IT-Sicherheit & Datenschutz

29.09.2022

DIGITAL
AGENTUR
BERLIN

Agenda

1. Vorstellung der DAB
2. Gefährdungslage
3. Begriffsbestimmungen
4. IT-Sicherheit im Unternehmen etablieren
5. Datenschutz für Startups
6. Fragerunde

Digitalagentur Berlin – Gemeinsam für Berlin

Als zentrale Koordinierungsstelle werden wir gemeinsam mit allen Stakeholdern die Digitalisierung vorantreiben und Berlin nachhaltig zukunftsfähig machen. Die DAB unterstützt die Berliner Unternehmen in jeder Phase ihrer digitalen Transformation.

100-prozentige Beteiligung der IBB Unternehmensverwaltung AöR sowie gefördert und finanziert vom Land Berlin.

BERLIN
Senatsverwaltung für Wirtschaft, Energie und Betriebe

Investitionsbank Berlin

Unsere Angebote

Förderung

Zur Finanzierung der Digitalisierung werden Förder- und Finanzierungsangebote vom Bund, vom Land und der EU für Unternehmen angeboten. Wir helfen Ihnen, die Angebote zu sortieren und zu bewerten, welches Finanzierungsinstrument für Ihr Vorhaben geeignet ist.

IT-Sicherheit

Wir sensibilisieren Berliner Unternehmen hinsichtlich IT-Sicherheit. Wir erklären, wie Sie schnell und effizient Ihr Unternehmen vor IT-Vorfällen und Hackern schützen können. Unser kostenfreies Angebot gilt allen Berliner Unternehmen.

Projekte

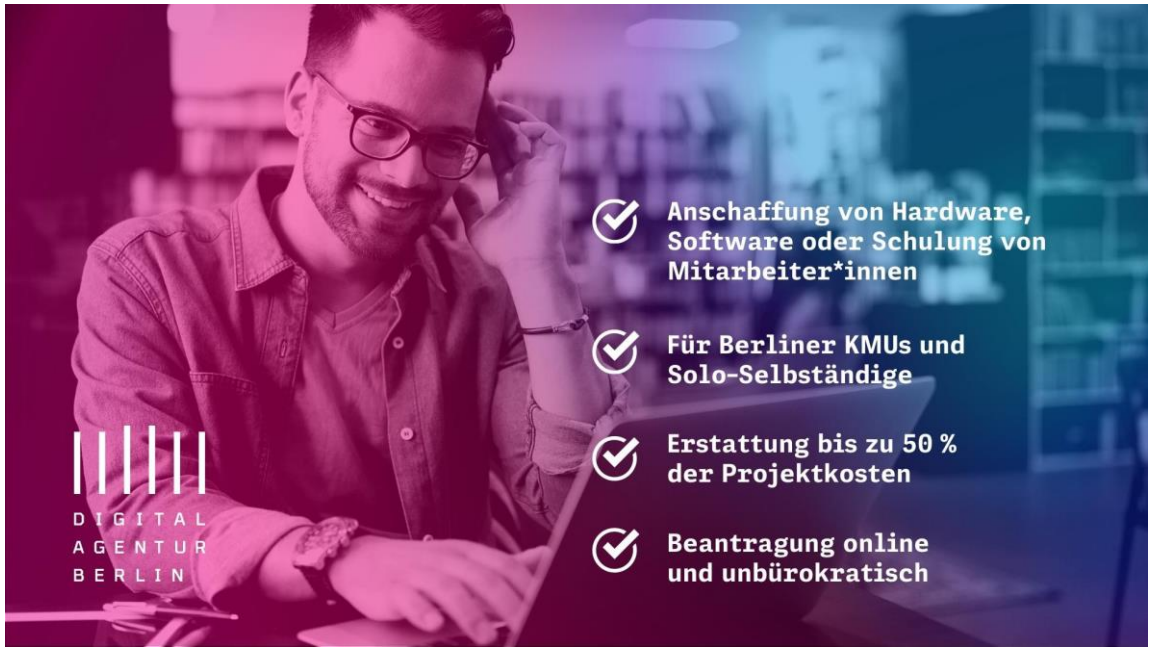
Wir bieten Berliner Unternehmen eine niedrigschwellige Möglichkeit zur Digitalisierung ihres Betriebs. Wir kooperieren dabei mit Berliner Hochschulen und Institutionen, wie zum Beispiel beim Projekt Digital+ der HTW.

Die Digitalprämie für Ihr Digitalisierungsprojekt

Die Digitalprämie soll finanzielle Anreize für kleine und mitteständische Berliner Unternehmen und Soloselbstständige schaffen, um in ihre digitale Transformation zu investieren.
Bis zu 17.000€ Zuschuss – 50% Prozent der Projektkosten werden erstattet.
Was darf gefördert werden?

1. Digitale Transformation von Arbeits-, Produktions- und Managementprozessen.
2. Einführung oder Verbesserung der betrieblichen IT-Sicherheit
3. Erwerb von digitalen Qualifikationen

ACHTUNG: Antragsstellende Betriebe müssen den Berliner Mindestlohn von 13€/h an ihre Beschäftigten.



digitalagentur.berlin/digitalpraemie

DIGITAL AGENTUR BERLIN

Cyberhotline für die Berliner Wirtschaft

Im Durchschnitt wird jedes dritte Unternehmen in Deutschland Ziel von Cyberangriffen. Insbesondere kleine und mittlere Unternehmen sind Ziel der zahlreichen Angriffe, die nicht selten existenzbedrohend sind. Mit einer zentralen Cyberhotline bekommen die Berliner Unternehmen die Möglichkeit, im Notfall umgehend erste Hilfe bei Angriffen auf ihre IT-Infrastruktur zu erhalten.

Das leistet die Cyberhotline

- zentrale Rufnummer für alle Berliner Unternehmen
- montags–freitags in der Zeit von 9–17 Uhr
- das Angebot kann reaktiv im Notfall genutzt werden
- schnelle Hilfe durch speziell ausgebildete Ersthelfer*innen
- Zugriff auf ein Netzwerk von privaten IT-Sicherheitsunternehmen
- Webinare ergänzen das Angebot

030 166 360 580

In Zusammenarbeit mit

it's BB
DAS IT-SICHERHEITSNETZWERK BERLIN-BRANDENBURG

digitalagentur.berlin/cyberhotline

Die Gefährdungslage

BSI Lagebericht 2021: „Die Bedrohung durch Cyber-Kriminelle steigt weiter an.“

+22%

144 Mio.

neue Schadsoftware-Varianten

KMUs

besonders anfällig für Bedrohungen

Homeoffice

bietet größere Angriffsfläche

Neuer Trend – Schweigegelderpressungen:

360%

mehr Daten-Leak-Seiten

Schwachstellen

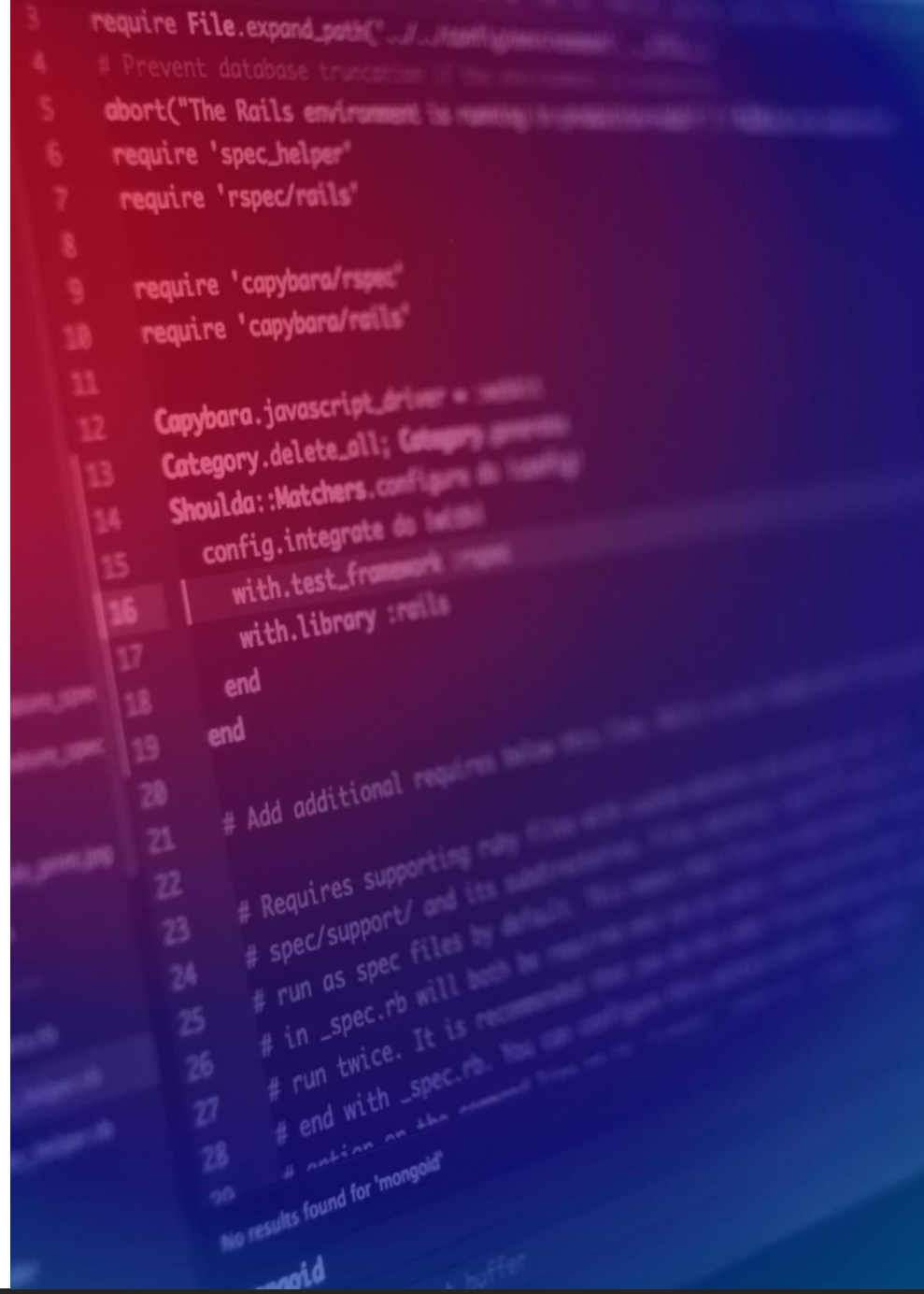
große Herausforderung

Quelle: „Die Lage der IT-Sicherheit in Deutschland 2021“, September 2021, Bundesamt für Sicherheit in der Informationstechnik (BSI) (Hrsg.), URL: https://www.bsi.bund.de/DE/Service-Navi/Publikationen/Lagebericht/lagebericht_node.html.

Cyberangriffe auf deutsche Unternehmen

Bitkom Studie 2022

- 9 von 10 Unternehmen werden Opfer von Datendiebstahl, Spionage und Sabotage
- Dadurch entsteht jährlich ein Schaden von 203 Mrd. Euro (2021: 223 Mrd.)
  - Davon lassen sich 52 Mrd. auf Angriffe im Homeoffice zurückführen (Institut der deutschen Wirtschaft)
- Organisierte Kriminalität nimmt zu



Quelle: https://www.bitkom.org/Presse/Presseinformation/Wirtschaftsschutz-2022, https://www.iwkoeln.de/presse/pressemitteilungen/barbara-engels-sicherheitsrisiko-homeoffice.html

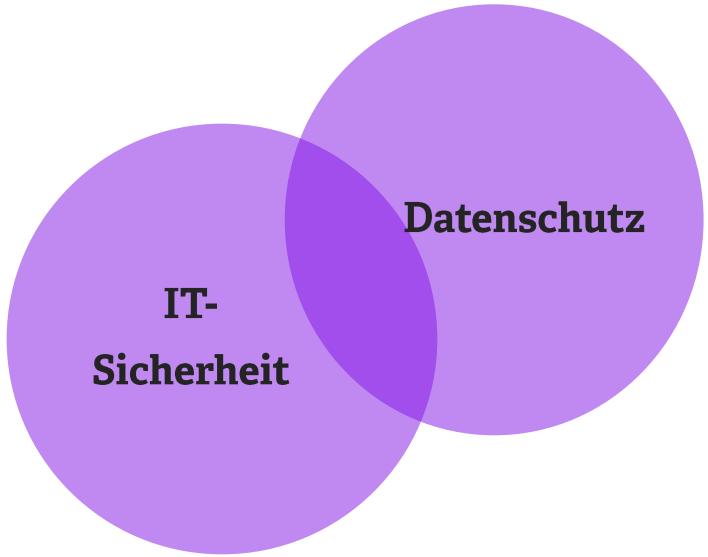
Begriffsbestimmungen

Aspekte der Informationssicherheit: IT-Sicherheit & Datenschutz

IT-Sicherheit

Schutz von IT-Systemen und den elektr. gespeicherten Informationen

Bezieht sich vorrangig auf technische Maßnahmen



Datenschutz

Schutz der personenbezogenen Daten

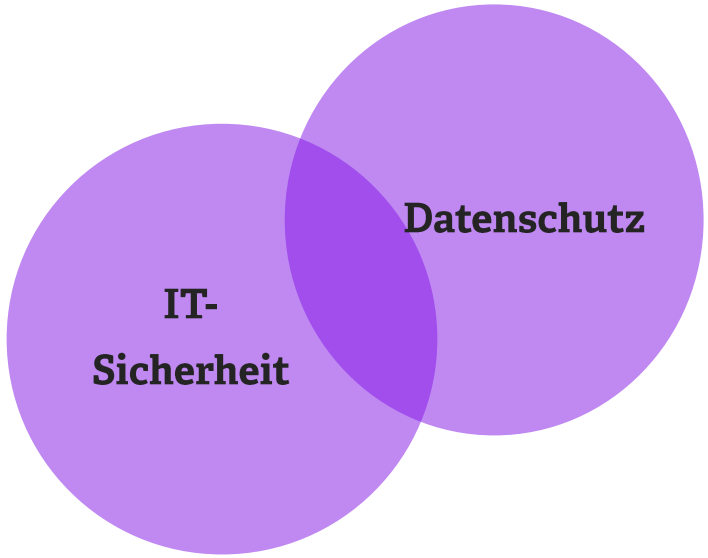
Grundlage ist das Prinzip der informationellen Selbstbestimmung

Sicherheit durch geeignete Maßnahmen erreichen

Ausgewählte Maßnahmen orientieren sich an dem eigenen angestrebten Sicherheitsniveau – abgeleitet vom Schutzniveau der Daten und Infrastruktur.

Informations-sicherheit

Der IT-Grundschutz vom BSI als Arbeitswerkzeug unterteilt in technische, infrastrukturelle, organisatorische und personelle Maßnahmen.



Datenschutz

TOMs- technisch organisatorische Maßnahmen

Unternehmen, die personenbezogene Daten verarbeiten, müssen diese Daten mit entsprechenden technischen und organisatorischen Maßnahmen schützen.

IT-Sicherheit im Unternehmen etablieren

Erste Schritte einleiten

1.

Verantwortlichkeiten festlegen

- IT-Sicherheit ist Chefsache
- Rollen festlegen: Wer ist für das Thema IT-Sicherheit verantwortlich?
- Im Falle eines Cybervorfalls: Meldewege
  - Welche Personen sind zu informieren (Geschäftsführung, IT-Leiter, Informationssicherheitsbeauftragte, Datenschutzbeauftragte, PR)

2.

Überblick über die eigene IT, Infrastruktur und Datenlage verschaffen

- Welche Systeme und Anwendungen sind im Unternehmen vorhanden?
- Nicht nur Software mit der jeweiligen Version auch Hardware (von PCs zu Druckern und Routern etc.) und vorhandene Lizenzen sollten berücksichtigt werden.
- Gibt es eine Dokumentation über Ihre Kommunikationsverbindungen?
- Überblick über Räumlichkeiten des Unternehmens und deren Absicherung
- Mit welchen Daten arbeitet das Unternehmen und welche Mitarbeitenden haben Zugriff auf welche Daten?

Ausgewählte Schutzmaßnahmen

- **Virenschutzprogramm & Firewall**
- Zutrittskontrollmaßnahmen
- Datensicherungen
- Updates
- Homeoffice-Richtlinie
- Passwort-Policy
- Notfallmanagement

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- **Zutrittskontrollmaßnahmen**
- Datensicherungen
- Updates
- Homeoffice-Richtlinie
- Passwort-Policy
- Notfallmanagement

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- **Datensicherungen**
- Updates
- Homeoffice-Richtlinie
- Passwort-Policy
- Notfallmanagement

Ausgewählte Schutzmaßnahmen

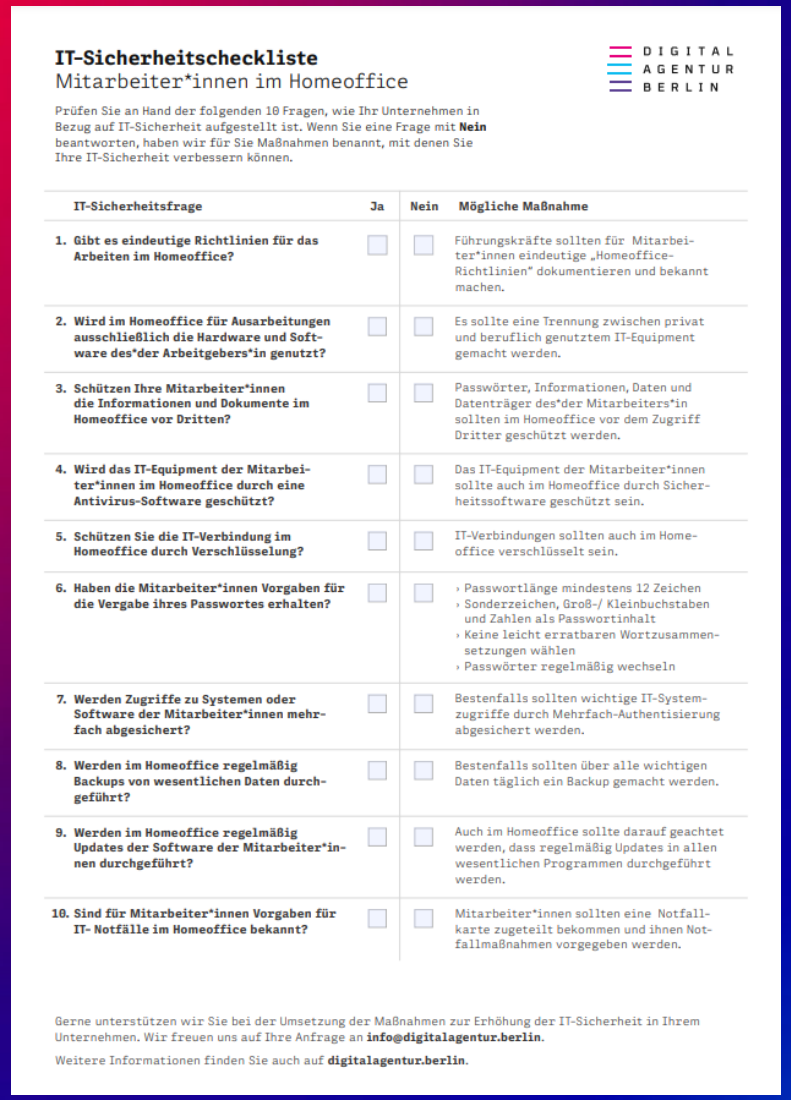
- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- Datensicherungen
- **Updates**
- Homeoffice-Richtlinie
- Passwort-Policy
- Notfallmanagement

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- Datensicherungen
- Updates
- **Homeoffice-Richtlinie**
- Passwort-Policy
- Notfallmanagement

Homeoffice & IT-Sicherheit

Nr.	Wichtigste Maßnahmen für Arbeit im Homeoffice
1	Richtlinien für Mitarbeiter*innen im Homeoffice
2	Trennung zwischen privatem und beruflichem IT-Equipment
3	Schutz von beruflichen Daten vor Dritten
4	Schutz des IT-Equipments durch Sicherheitssoftware
5	Absichern der IT-Verbindung des Homeoffices durch Verschlüsselung
6	Standardisierte sichere Passwort-Vorgaben
7	Mehrfach-Absicherung der Zugänge zu IT-Systemen
8	Regelmäßige Backups von Daten
9	Regelmäßige Software-Updates im Homeoffice
10	Vorgaben für Mitarbeiter*innen im IT-Notfall



IT-Sicherheitscheckliste
Mitarbeiter*innen im Homeoffice

DIGITAL AGENTUR BERLIN

Prüfen Sie an Hand der folgenden 10 Fragen, wie Ihr Unternehmen in Bezug auf IT-Sicherheit aufgestellt ist. Wenn Sie eine Frage mit **Nein** beantworten, haben wir für Sie Maßnahmen benannt, mit denen Sie Ihre IT-Sicherheit verbessern können.

	IT-Sicherheitsfrage	Ja	Nein	Mögliche Maßnahme
1.	**Gibt es eindeutige Richtlinien für das Arbeiten im Homeoffice?**	☐	☐	Führungskräfte sollten für Mitarbeiter*innen eindeutige „Homeoffice-Richtlinien" dokumentieren und bekannt machen.
2.	**Wird im Homeoffice für Ausarbeitungen ausschließlich die Hardware und Software des*der Arbeitgebers*in genutzt?**	☐	☐	Es sollte eine Trennung zwischen privat und beruflich genutztem IT-Equipment gemacht werden.
3.	**Schützen Ihre Mitarbeiter*innen die Informationen und Dokumente im Homeoffice vor Dritten?**	☐	☐	Passwörter, Informationen, Daten und Datenträger des*der Mitarbeiters*in sollten im Homeoffice vor dem Zugriff Dritter geschützt werden.
4.	**Wird das IT-Equipment der Mitarbeiter*innen im Homeoffice durch eine Antivirus-Software geschützt?**	☐	☐	Das IT-Equipment der Mitarbeiter*innen sollte auch im Homeoffice durch Sicherheitssoftware geschützt sein.
5.	**Schützen Sie die IT-Verbindung im Homeoffice durch Verschlüsselung?**	☐	☐	IT-Verbindungen sollten auch im Homeoffice verschlüsselt sein.
6.	**Haben die Mitarbeiter*innen Vorgaben für die Vergabe ihres Passwortes erhalten?**	☐	☐	› Passwortlänge mindestens 12 Zeichen › Sonderzeichen, Groß-/ Kleinbuchstaben und Zahlen als Passwortinhalt › Keine leicht erratbaren Wortzusammensetzungen wählen › Passwörter regelmäßig wechseln
7.	**Werden Zugriffe zu Systemen oder Software der Mitarbeiter*innen mehrfach abgesichert?**	☐	☐	Bestenfalls sollten wichtige IT-Systemzugriffe durch Mehrfach-Authentisierung abgesichert werden.
8.	**Werden im Homeoffice regelmäßig Backups von wesentlichen Daten durchgeführt?**	☐	☐	Bestenfalls sollten über alle wichtigen Daten täglich ein Backup gemacht werden.
9.	**Werden im Homeoffice regelmäßig Updates der Software der Mitarbeiter*innen durchgeführt?**	☐	☐	Auch im Homeoffice sollte darauf geachtet werden, dass regelmäßig Updates in allen wesentlichen Programmen durchgeführt werden.
10.	**Sind für Mitarbeiter*innen Vorgaben für IT- Notfälle im Homeoffice bekannt?**	☐	☐	Mitarbeiter*innen sollten eine Notfallkarte zugeteilt bekommen und ihnen Notfallmaßnahmen vorgegeben werden.

Gerne unterstützen wir Sie bei der Umsetzung der Maßnahmen zur Erhöhung der IT-Sicherheit in Ihrem Unternehmen. Wir freuen uns auf Ihre Anfrage an **info@digitalagentur.berlin**.

Weitere Informationen finden Sie auch auf **digitalagentur.berlin**.

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- Datensicherungen
- Updates
- Homeoffice-Richtlinie
- **Passwort-Policy**
- Notfallmanagement

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- Datensicherungen
- Updates
- Homeoffice-Richtlinie
- Passwort-Policy
- **Notfallmanagement**

Der DAB-Notfallplan im Falle eines Cyberangriffes

Ausgewählte Schutzmaßnahmen

- Virenschutzprogramm & Firewall
- Zutrittskontrollmaßnahmen
- Datensicherungen
- Updates
- Homeoffice-Richtlinie
- Passwort-Policy
- Notfallmanagement

Augenmerk: Prävention durch Schulung von Awareness

Grundlage für eine erfolgreiche Umsetzung: Mitarbeitende sensibilisieren

1. Verständnis für Maßnahmen schaffen

2. Mitarbeitende übernehmen mehr IT-Sicherheits-verantwortung

3. regelmäßige Sensibilisierungs-maßnahmen

IT-Sicherheitschecklisten der DAB

Unternehmen

- Organisation
- Prozesse
- Mitarbeiter*innen
- Homeoffice

Technik

- Hardware
- Software
- Verbindungen

Prozesse

- DSGVO
- Risikoanalyse
- Schutzbedarfsanalyse
- ITS-Bericht

digitalagentur.berlin/angebote-it-sicherheit/

Datenschutz für Gründer*innen

Achten Sie darauf, dass auch Ihre IT **von Anfang** an datenschutzkonform eingerichtet ist.

Ein Datenschutzvorfall ist **meldepflichtig** und kann früh das Vertrauen der Kunden verspielen.

Deswegen: „**Privacy First**“ - Gründer müssen sich schon in der Seeding-Phase mit dem Datenschutz vertraut machen.

Wenn Sie eigene Produkte wie Apps oder Online-Shops entwickeln, müssen Sie der Grundregel „**Privacy by Design**“ folgen.

Die frühzeitige Benennung eines **Datenschutzbeauftragten** ist in jedem Fall ratsam – unabhängig davon, ob Sie dazu gesetzlich verpflichtet sind.

Nehmen Sie einen **Datenschutz-Dienstleister** in Anspruch, der Ihnen in den unterschiedlichen Unternehmensphasen die passende Expertise bietet.

Internationale Expansion bringt neue und komplexe Herausforderungen im Datenschutz mit sich. Holen Sie sich das entsprechende Know-how ins Boot.

Fazit für Gründer*innen

Denken Sie IT-Sicherheit von Anfang an mit!
Es ist schwieriger, bestehende Prozesse und Gewohnheiten zu ändern, als diese gleich zu Beginn richtig zu machen.

IT-Sicherheit

Denken Sie nicht nur an Antivirus-Software und Firewall, sondern auch an IT-sichere Arbeitsprozesse.

Ein IT-Sicherheitsvorfall kann den Traum des eigenen Unternehmen beenden, bevor er richtig begonnen hat.

Schulen Sie Ihre Mitarbeiter in Sachen IT-Sicherheit.

Datenschutz

Stellen Sie sicher, dass Ihre Prozesse von Anfang an DSGVO-konform sind. Wenn Sie mit großen Mengen an personenbezogenen Daten Arbeiten, lohnt es sich, einen Spezialisten hinzuzuziehen.

Ab 20 Mitarbeitern ist i.d.R. ein Datenschutzbeauftragter verpflichtend.

Ein Datenschutzvorfall kann nicht nur teuer werden, Sie verspielen so auch das Vertrauen Ihrer Kunden und riskieren einen irreparablen Image-Schaden.

Nehmen Sie Hilfe an!

Nehmen Sie die kostenlosen Orientierungsangebote der Digitalagentur Berlin in Anspruch.

Lassen Sie Ihre IT-Infrastruktur von spezialisierten Dienstleister auf ihre Widerstandsfähigkeit testen – eine Dienstleistung, die oftmals förderfähig ist.

Wir beantworten Ihre Fragen

Ihre Ansprechpartnerinnen

Moritz Vernier

Projektmanager Netzwerk- und Kund*innenmanagement

moritz.vernier@digitalagentur.berlin

Vanessa Schneeweiß

Projektmanagerin IT-Sicherheit

vanessa.schneeweiss@digitalagentur.berlin

digitalagentur.berlin

/digitalagenturberlin

/DABGmbH