INTELLIGENT SECURITY HANDWERK

Weiterbildungsreihe für Handwerksbetriebe

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

Mittelstand-Digital

Inhaltsverzeichnis

Inhaltsverzeichnis

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Inhaltsverzeichnis

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

Inhaltsverzeichnis

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

1. Grundlagen der Datensicherheit

Definition Datensicherheit

Datensicherheit bedeutet, digitale Daten vor destruktiven Kräften und vor unerwünschten Aktionen unbefugter Benutzer, wie z. B. einem Cyberangriff oder einer Datenschutzverletzung, zu schützen.

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

1. Grundlagen der Datensicherheit

Unterschied Datenschutz Datensicherheit

Beim **Datenschutz** geht es um die rechtlichen Fragen, unter welchen Voraussetzungen personenbezogene Daten erhoben, verarbeitet oder genutzt werden dürfen. Die **Datensicherheit** befasst sich mit dem generellen Schutz von Daten, unabhängig davon, ob ein Personenbezug besteht oder nicht.

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

1. Grundlagen der Datensicherheit

Schutz persönlicher Daten: Persönliche Informationen wie Namen, Adressen, Geburtsdaten, Sozialversicherungsnummern und finanzielle Daten sind wertvoll und können missbraucht werden, wenn sie in die falschen Hände geraten. Datensicherheit schützt diese Informationen vor Identitätsdiebstahl und anderen Formen des Missbrauchs.

Vertraulichkeit bewahren: Unternehmen und Organisationen müssen die Vertraulichkeit sensibler Daten, wie z.B. Geschäftsgeheimnisse, Kundeninformationen und geistiges Eigentum, gewährleisten. Datenlecks können zu erheblichen finanziellen Verlusten und einem Verlust des Vertrauens führen.

Einhaltung gesetzlicher Vorschriften: Viele Branchen unterliegen strengen Datenschutzgesetzen und -vorschriften, wie z.B. der DSGVO in der EU. Die Nichteinhaltung dieser Vorschriften kann zu hohen Geldstrafen und rechtlichen Konsequenzen führen.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

1. Grundlagen der Datensicherheit

Warum Datensicherheit wichtig ist

Schutz vor Cyberkriminalität: Die Bedrohung durch Cyberangriffe, wie Phishing, Ransomware und Malware, nimmt ständig zu. Datensicherheitsmaßnahmen helfen, solche Angriffe abzuwehren und die Integrität der Systeme und Daten zu bewahren.

Wirtschaftliche Stabilität: Datenverluste können zu erheblichen finanziellen Einbußen führen. Neben den direkten Kosten für die Behebung von Datenschutzverletzungen können auch langfristige Schäden wie der Verlust von Kundenvertrauen und der Unternehmensreputation entstehen.

Betriebliche Kontinuität: Datenverlust oder -kompromittierung kann den Betrieb von Unternehmen erheblich beeinträchtigen. Sicherungs- und Wiederherstellungspläne sind entscheidend, um die Geschäftskontinuität zu gewährleisten und Ausfallzeiten zu minimieren.

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

1. Grundlagen der Datensicherheit
Warum Datensicherheit wichtig ist

Vermeidung von Reputationsschäden: Unternehmen, die Opfer von Datenlecks werden, riskieren erhebliche Reputationsschäden. Das Vertrauen der Kunden und Partner kann verloren gehen, was langfristig den Geschäftserfolg beeinträchtigen kann.

Vertraulichkeit und Integrität der Kommunikation: Sichere Kommunikationskanäle sind entscheidend, um sicherzustellen, dass Informationen nicht abgefangen oder manipuliert werden können. Dies gilt sowohl für die interne Kommunikation innerhalb eines Unternehmens als auch für die externe Kommunikation mit Kunden und Partnern.

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

1. Grundlagen der Datensicherheit

Fazit Datensicherheit

Durch die Implementierung robuster Datensicherheitsmaßnahmen können Einzelpersonen und Organisationen ihre sensiblen Informationen schützen, regulatorische Anforderungen erfüllen und sich gegen die wachsende Bedrohung durch Cyberkriminalität wappnen.

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

1. Grundlagen der Datensicherheit

Fazit Datensicherheit

Ziel der Datensicherheit ist es, die Integrität (Richtigkeit), Vertraulichkeit und Verfügbarkeit von Daten sicherzustellen. Dies wird durch eine Vielzahl von Maßnahmen erreicht, darunter:

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

1. Grundlagen der Datensicherheit

Maßnahmen für Datensicherheit

Technische Maßnahmen: Einsatz von Firewalls, Verschlüsselung, Antiviren-Software und sicheren Netzwerken.

Organisatorische Maßnahmen: Implementierung von Sicherheitsrichtlinien, Zugriffsrechten und regelmäßigen Sicherheitsüberprüfungen.

Physische Maßnahmen: Schutz der Hardware durch sichere Standorte, Überwachung und Zugangskontrollen.

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

1. Grundlagen der Datensicherheit

Bedrohungen der Datensicherheit

Malware: Schadsoftware wie Viren, Trojaner, Ransomware und Spyware, die Systeme infizieren und Daten beschädigen, stehlen oder verschlüsseln können.

Phishing: Angriffe, bei denen Betrüger versuchen, sensible Informationen wie Benutzernamen, Passwörter und Kreditkartennummern durch Täuschung zu erlangen. Dies geschieht oft über gefälschte E-Mails oder Webseiten.

Hacking: Unbefugter Zugriff auf Computersysteme, oft durch das Ausnutzen von Sicherheitslücken oder durch Brute-Force-Angriffe, um Daten zu stehlen oder Systeme zu kompromittieren.

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

1. Grundlagen der Datensicherheit

Bedrohungen der Datensicherheit

Insider-Bedrohungen: Risiken, die von aktuellen oder ehemaligen Mitarbeitern, Auftragnehmern oder Geschäftspartnern ausgehen, die absichtlich oder versehentlich sensible Daten gefährden.

Denial-of-Service (DoS)-Angriffe: Angriffe, die darauf abzielen, Dienste durch Überlastung der Netzwerkressourcen lahmzulegen, was zu einem Ausfall von Diensten und dem Verlust von Datenzugriff führen kann.

Man-in-the-Middle (MitM)-Angriffe: Angriffe, bei denen ein Angreifer die Kommunikation zwischen zwei Parteien abfängt und möglicherweise verändert, um vertrauliche Informationen zu stehlen oder Daten zu manipulieren.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

Mittelstand-Digital

1. Grundlagen der Datensicherheit

Bedrohungen der Datensicherheit

Zero-Day-Exploits: Angriffe, die Sicherheitslücken ausnutzen, die dem Softwarehersteller und der Öffentlichkeit noch nicht bekannt sind. Solche Lücken sind besonders gefährlich, da es keine verfügbaren Patches gibt.

Social Engineering: Techniken, bei denen Angreifer menschliche Interaktionen manipulieren, um vertrauliche Informationen zu erlangen. Beispiele sind Telefonbetrug und physische Manipulation.

Verlust oder Diebstahl von Geräten: Mobile Geräte, Laptops oder externe Speicher, die verloren gehen oder gestohlen werden, können sensible Daten gefährden, insbesondere wenn sie nicht verschlüsselt sind.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

1. Grundlagen der Datensicherheit

Bedrohungen der Datensicherheit

Unzureichende Zugangskontrollen: Wenn Zugriffsrechte nicht angemessen verwaltet werden, können unbefugte Personen auf sensible Informationen zugreifen.

Ungepatchte Software: Systeme, die nicht regelmäßig aktualisiert werden, sind anfällig für bekannte Sicherheitslücken, die von Angreifern ausgenutzt werden können.

Cloud-Sicherheitsprobleme: Risiken, die mit der Speicherung und Verarbeitung von Daten in der Cloud verbunden sind, wie z.B. Fehlkonfigurationen, mangelnde Verschlüsselung und gemeinsame Ressourcen.

I**nternet der Dinge (IoT)-Schwachstellen**: Unsichere IoT-Geräte, die in Netzwerke integriert sind, können als Einstiegspunkte für Angriffe dienen.

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

1. Grundlagen der Datensicherheit
Klassifizierung von Daten

Öffentliche Daten:

Beschreibung: Diese Daten sind frei zugänglich und können ohne Einschränkungen weitergegeben werden.

Beispiele: Veröffentlichte Berichte, Pressemitteilungen, Marketingmaterialien.

Schutzmaßnahmen: Geringe Schutzanforderungen, da keine sensiblen Informationen enthalten sind.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

1. Grundlagen der Datensicherheit

Klassifizierung von Daten

Interne Daten:

Beschreibung: Daten, die für den internen Gebrauch innerhalb einer Organisation bestimmt sind und nicht für die Öffentlichkeit zugänglich sein sollen.

Beispiele: Interne Richtlinien, Mitarbeiterinformationen (ohne sensible persönliche Daten), Geschäftsinterna.

Schutzmaßnahmen: Zugangskontrollen, interne IT-Sicherheitsrichtlinien.

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

1. Grundlagen der Datensicherheit

Klassifizierung von Daten

Vertrauliche Daten:

Beschreibung: Daten, deren Zugang auf bestimmte Gruppen innerhalb der Organisation beschränkt ist, da ihre Offenlegung potenziell Schaden anrichten könnte.

Beispiele: Kundenlisten, Geschäftspartnerinformationen, interne Strategiedokumente.

Schutzmaßnahmen: Strenge Zugangskontrollen, Verschlüsselung bei der Speicherung und Übertragung, regelmäßige Überprüfungen der Zugriffsrechte.

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

1. Grundlagen der Datensicherheit

Klassifizierung von Daten

Geheime Daten:

Beschreibung: Daten, die besonders sensibel sind und deren unautorisierter Zugriff erhebliche Schäden verursachen könnte.

Beispiele: Geschäftsgeheimnisse, vertrauliche Verträge, Finanzdaten, medizinische Daten.

Schutzmaßnahmen: Höchste Sicherheitsvorkehrungen wie starke Verschlüsselung, Multi-Faktor-Authentifizierung, regelmäßige Sicherheitsaudits.

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

1. Grundlagen der Datensicherheit

Klassifizierung von Daten

Hochsensible oder persönliche Daten:

Beschreibung: Daten, die personenbezogene Informationen enthalten und deren Schutz gemäß Datenschutzgesetzen wie der DSGVO besonders wichtig ist.

Beispiele: Sozialversicherungsnummern, Kreditkartendaten, Gesundheitsdaten, biometrische Daten.

Schutzmaßnahmen: Sehr strenge Schutzmaßnahmen, einschließlich Anonymisierung oder Pseudonymisierung, Einwilligung der betroffenen Personen, regelmäßige Schulungen der Mitarbeiter im Datenschutz.

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

2. Technologische Grundlagen
Begrifflichkeiten

Firewalls: Hardware- oder Softwarelösungen, die den ein- und ausgehenden Datenverkehr basierend auf festgelegten Sicherheitsregeln überwachen und steuern.

Antivirus- und Anti-Malware-Software: Programme, die schädliche Software identifizieren, blockieren und entfernen können. Moderne Lösungen verwenden oft maschinelles Lernen, um unbekannte Bedrohungen zu erkennen.

Verschlüsselung: Der Prozess, Daten in einen unleserlichen Code zu verwandeln, um sicherzustellen, dass nur autorisierte Parteien sie entschlüsseln und lesen können. Asymmetrische Verschlüsselung (z.B. RSA) und symmetrische Verschlüsselung (z.B. AES) sind weit verbreitete Methoden.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

2. Technologische Grundlagen
Begrifflichkeiten

Intrusion Detection und Prevention Systeme (IDPS): Systeme, die Netzwerke und Systeme auf verdächtige Aktivitäten überwachen (Detection) und Maßnahmen ergreifen, um Angriffe zu verhindern (Prevention).

Multi-Faktor-Authentifizierung (MFA): Eine Methode, bei der für den Zugriff auf ein System mehrere Authentifizierungsfaktoren erforderlich sind, z.B. ein Passwort und ein zusätzlicher Code von einer App.

Virtual Private Networks (VPN): Technologien, die eine sichere, verschlüsselte Verbindung über ein weniger sicheres Netzwerk wie das Internet bereitstellen.

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

Mittelstand-Digital

2. Technologische Grundlagen

Moderne Entwicklungen + Herausforderungen

Künstliche Intelligenz und maschinelles Lernen: Diese Technologien werden zunehmend sowohl von Angreifern als auch von Verteidigern genutzt. Sie können helfen, Anomalien zu erkennen und Bedrohungen erkennen, stellen aber auch neue Herausforderungen dar.

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

2. Technologische Grundlagen
Moderne Entwicklungen + Herausforderungen

Cloud-Sicherheit: Die Verlagerung von Daten und Diensten in die Cloud erfordert spezifische Sicherheitsmaßnahmen wie 2-Faktor-Authentifizierung, Zugriffsbeschränkungen und datenorientierte Verschlüsselung.

IoT-Sicherheit (Internet der Dinge): Mit der zunehmenden Vernetzung von Geräten steigt die Notwendigkeit, diese Geräte vor Cyberangriffen zu schützen. Schwachstellen in IoT-Geräten können zu weitreichenden Sicherheitsproblemen führen.

Verbesserte Verschlüsselungsmethoden: In naher Zukunft könnten neue Verschlüsselungsmethoden eine wichtige Rolle beim Schutz vor Angriffen spielen, die herkömmliche Verschlüsselungsverfahren überwinden könnten.

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

Mittelstand-Digital

2. Technologische Grundlagen
Best Practices zur Datensicherheit

Regelmäßige Updates und Patches: Software und Systeme sollten regelmäßig aktualisiert werden, um bekannte Sicherheitslücken zu schließen.

Sicherheitsbewusstsein schulen: Mitarbeiter sollten regelmäßig in den neuesten Sicherheitstechniken und -bedrohungen geschult werden.

Backup und Wiederherstellung: Regelmäßige Backups von wichtigen Daten und eine getestete Wiederherstellungsstrategie können im Falle eines Angriffs oder Datenverlusts entscheidend sein.

Zugriffssteuerung: Implementierung des Prinzips der geringsten Privilegien, um sicherzustellen, dass Benutzer nur Zugriff auf die Daten und Systeme haben, die sie benötigen.

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

3. Phishing-Prävention

Phishing ist eine Form von Cyberkriminalität, bei der Angreifer versuchen, sensible Informationen wie Passwörter, Kreditkartendaten oder persönliche Identifikationsnummern (PINs) zu stehlen, indem sie sich als vertrauenswürdige Entität ausgeben. Die Prävention von Phishing-Angriffen ist entscheidend, um die Sicherheit sowohl für Einzelpersonen als auch für Unternehmen zu gewährleisten.

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

3. Phishing-Prävention
Bewusstsein und Schulung

Sensibilisierung: Schulen Sie Mitarbeiter und Endnutzer regelmäßig, damit sie Phishing-Angriffe erkennen können. Dies umfasst das Erkennen von verdächtigen E-Mails, Links und Anhängen.

Sicherheitsbewusstsein: Stellen Sie sicher, dass alle im Unternehmen wissen, wie wichtig es ist, persönliche Daten nicht leichtfertig weiterzugeben.

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

3. Phishing-Prävention

Technische Maßnahmen

E-Mail-Filter: Verwenden Sie E-Mail-Sicherheitslösungen, die verdächtige E-Mails erkennen und blockieren können.

Multi-Faktor-Authentifizierung (MFA): Implementieren Sie MFA, um zusätzliche Sicherheitsschichten hinzuzufügen. Selbst wenn Anmeldedaten gestohlen werden, bleibt der Zugang gesperrt.

SSL/TLS-Verschlüsselung: Stellen Sie sicher, dass alle sensiblen Datenübertragungen verschlüsselt sind, um Man-in-the-Middle-Angriffe zu verhindern.

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

3. Phishing-Prävention
Identifizierung und Umgang mit Phishing-E-Mails

Verdächtige Absender: Überprüfen Sie die E-Mail-Adresse des Absenders genau. Phishing-E-Mails kommen oft von Adressen, die vertrauenswürdigen Absendern ähneln, aber leicht abgeändert sind.

Dringlichkeit und Bedrohung: Phishing-E-Mails enthalten oft dringende Nachrichten oder drohen mit negativen Konsequenzen, um die Zielperson zur schnellen Reaktion zu verleiten.

Rechtschreibung und Grammatik: Viele Phishing-E-Mails enthalten Rechtschreib- oder Grammatikfehler, da sie oft maschinell übersetzt oder von Nicht-Muttersprachlern erstellt werden.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

3. Phishing-Prävention
Sicherer Umgang mit Links und Anhängen

Links überprüfen: Bewegen Sie den Mauszeiger über Links, um die tatsächliche URL anzuzeigen, bevor Sie darauf klicken. Stellen Sie sicher, dass die Adresse korrekt ist und zu einer vertrauenswürdigen Domain gehört.

Anhänge nicht öffnen: Öffnen Sie keine Anhänge aus unerwarteten E-Mails, insbesondere wenn sie von unbekannten Absendern stammen oder verdächtig erscheinen.

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

3. Phishing-Prävention
Verdachtsfälle melden

Meldeprozess: Richten Sie klare Prozesse ein, wie verdächtige E-Mails oder Phishing-Versuche intern gemeldet werden können.

Reaktionsteams: Haben Sie ein IT-Sicherheitsteam oder eine zuständige Abteilung, die auf Phishing-Vorfälle schnell reagieren kann.

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

3. Phishing-Prävention
Regelmäßige Software-Updates

Patch-Management: Stellen Sie sicher, dass alle Systeme und Softwarelösungen regelmäßig aktualisiert werden, um Sicherheitslücken zu schließen, die von Phishing-Angreifern ausgenutzt werden könnten.

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

3. Phishing-Prävention
Sicherheitsbewusste Kultur fördern

Verantwortungsbewusstsein: Fördern Sie eine Kultur, in der alle Mitarbeiter Verantwortung für die Sicherheit übernehmen und aktiv dazu beitragen, Phishing-Risiken zu minimieren.

Offene Kommunikation: Ermutigen Sie zu einer offenen Kommunikation über potenzielle Sicherheitsbedrohungen ohne Angst vor Sanktionen, damit Vorfälle schnell gemeldet werden.

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

3. Phishing-Prävention

Diese Präventionsmaßnahmen sind entscheidend, um Phishing-Angriffe zu verhindern oder ihre Auswirkungen zu minimieren. Eine Kombination aus technologischem Schutz, regelmäßiger Schulung und einer sicherheitsbewussten Kultur ist der Schlüssel zum Schutz vor Phishing.

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

4. Sichere Passwörter und Zugriffskontrolle

Bedeutung sicherer Passwörter:

Schutz vor unbefugtem Zugriff:

Passwörter sind die erste Verteidigungslinie gegen unbefugten Zugriff auf persönliche und berufliche Daten. Ein starkes Passwort schützt vor Datenlecks, Identitätsdiebstahl und anderen Cyberangriffen.

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

4. Sichere Passwörter und Zugriffskontrolle
Cyberangriffe und Brute-Force-Attacken:

Schwache Passwörter können leicht durch Brute-Force-Angriffe oder durch Wörterbuchangriffe geknackt werden.

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

4. Sichere Passwörter und Zugriffskontrolle

Eigenschaften eines sicheren Passworts:

Länge: Ein Passwort sollte mindestens 12–16 Zeichen lang sein.

Komplexität: Ein sicheres Passwort enthält eine Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen.

Kein Bezug zu persönlichen Informationen: Vermeiden Sie Passwörter, die mit Ihrem Namen, Geburtsdatum oder anderen leicht zu erratenden Informationen in Verbindung stehen.

Keine Wiederverwendung von Passwörtern: Jedes Konto sollte ein einzigartiges Passwort haben, um zu verhindern, dass ein kompromittiertes Passwort Zugang zu mehreren Konten ermöglicht.

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

4. Sichere Passwörter und Zugriffskontrolle

Techniken zur Erstellung und Verwaltung sicherer Passwörter

Passwort-Manager: Verwenden Sie Passwort-Manager, um starke Passwörter zu generieren, zu speichern und automatisch auszufüllen. Das reduziert das Risiko, schwache oder wiederverwendete Passwörter zu verwenden.

Passphrasen: Eine Passphrase ist eine Folge von Wörtern oder ein Satz, der schwer zu erraten ist, aber leicht zu merken. Sie bieten eine Balance zwischen Sicherheit und Benutzerfreundlichkeit.

Zwei-Faktor-Authentifizierung (2FA): Diese fügt eine zusätzliche Sicherheitsebene hinzu, indem sie einen zweiten Faktor (z.B. ein Einmalpasswort auf einem Mobilgerät) erfordert

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

4. Sichere Passwörter und Zugriffskontrolle

Best Practices für die Zugriffskontrolle

Minimaler Zugriff (Principle of Least Privilege): Nutzer sollten nur Zugriff auf die Informationen und Systeme haben, die sie für ihre Arbeit benötigen. Dies reduziert die Gefahr von Insider-Bedrohungen und minimiert den Schaden bei einem Sicherheitsvorfall.

Regelmäßige Überprüfung von Zugriffsrechten: Zugriffsrechte sollten regelmäßig überprüft und aktualisiert werden, um sicherzustellen, dass nur autorisierte Personen Zugriff auf sensible Daten haben.

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

4. Sichere Passwörter und Zugriffskontrolle

Best Practices für die Zugriffskontrolle

Protokollierung und Überwachung: Die Aktivitäten der Nutzer sollten protokolliert und überwacht werden, um verdächtige Zugriffe oder Anomalien frühzeitig zu erkennen.

Rollenbasierte Zugriffskontrolle (RBAC): Hierbei wird der Zugriff basierend auf der Rolle des Benutzers innerhalb der Organisation gewährt, was die Verwaltung vereinfacht und die Sicherheit erhöht.

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

4. Sichere Passwörter und Zugriffskontrolle

Schutz vor Social Engineering

Bewusstseinsschulung: Regelmäßige Schulungen für Mitarbeiter über die Gefahren von Social Engineering, Phishing und anderen Manipulationstechniken.

Verifizierungsmethoden:
Vor der Herausgabe von sensiblen Informationen sollten Verifizierungsmethoden angewendet werden, um sicherzustellen, dass der Anfragende tatsächlich berechtigt ist.

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

4. Sichere Passwörter und Zugriffskontrolle

Reaktionen auf Sicherheitsverletzungen

Sofortige Passwortänderung: Im Falle eines Verdachts auf einen Sicherheitsvorfall sollten betroffene Passwörter sofort geändert werden.

Kontrollierte Zugangssperre: Wenn ein unbefugter Zugriff festgestellt wird, sollte der Zugang umgehend gesperrt werden, um weiteren Schaden zu verhindern.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

4. Sichere Passwörter und Zugriffskontrolle

Fazit

Diese Inhalte bieten eine solide Grundlage für ein Verständnis der Bedeutung sicherer Passwörter und effektiver Zugriffskontrollen, sowie für die Umsetzung von Best Practices in diesen Bereichen.

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

5. Sicherer Umgang mit mobilen Geräten

Der sichere Umgang mit mobilen Geräten ist essenziell, um die Datensicherheit zu gewährleisten. Mobile Geräte wie Smartphones und Tablets sind oft Ziel von Cyberangriffen, da sie eine Fülle an sensiblen Daten enthalten.

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

5. Sicherer Umgang mit mobilen Geräten

1. Geräteschutz und Authentifizierung

Passwörter und PINs: starke, einzigartige Passwörter oder PINs verwenden, um den Zugriff auf das Gerät zu schützen. Eine Zwei-Faktor-Authentifizierung (2FA) bietet zusätzlichen Schutz.

Biometrische Sicherheit: Falls möglich, Fingerabdruckscanner oder Gesichtserkennung als zusätzliche Sicherheitsmaßnahme nutzen.

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

5. Sicherer Umgang mit mobilen Geräten

2. Verschlüsselung

Geräteverschlüsselung: Sicherstellen, dass das Gerät verschlüsselt ist, sodass im Falle eines Verlusts oder Diebstahls niemand auf Daten zugreifen kann.

Datenübertragung: verschlüsselte Verbindungen (z.B. VPNs, HTTPS) verwenden, um sensible Daten zu übertragen.

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

5. Sicherer Umgang mit mobilen Geräten

Viele neuere Geräte verfügen mittlerweile über eine Option zur Speichergrundverschlüsselung. Dies ist eine Verschlüsselungstechnik, die auf dem jeweiligen Gerät bereits integriert ist und das komplette Gerät inklusive gespeicherter Daten verschlüsselt. Ist diese aktiviert, können die Benutzerdaten in der Regel noch nicht einmal mit erheblichen Aufwänden, einem entsprechenden Hardwarelabor und tiefem Detailwissen lesbar gemacht werden.

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

5. Sicherer Umgang mit mobilen Geräten

Die Speichergrundverschlüsselung setzt in der Regel ein Einschalt- bzw. Display-Kennwort voraus. Ob und welches Verschlüsselungsverfahren auf Smartphones verfügbar ist, ist hersteller- und versionsabhängig. Dies betrifft ebenso deren Einstellung bzw. Aktivierung, welche unter anderem dem Gerätehandbuch entnehmbar sind. Wenn Sie sich nicht sicher sind, ob Ihr Gerät über eine Speichergrundverschlüsselung verfügt, erkundigen Sie sich bei unterschiedlichen Quellen über die Verschlüsselungsmöglichkeiten oder wenden Sie sich direkt an den Hersteller.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

5. Sicherer Umgang mit mobilen Geräten

3. Aktualisierungen und Patches

Regelmäßige Updates: Betriebssystem und installierte Apps immer auf dem neuesten Stand halten, um bekannte Sicherheitslücken zu schließen.

Automatische Updates: Automatische Updates aktivieren, um sicherzustellen, dass du die neuesten Sicherheitsverbesserungen erhältst.

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

Mittelstand-Digital

5. Sicherer Umgang mit mobilen Geräten

4. Sichere Netzwerke

Vermeidung öffentlicher WLANs: Öffentliche WLANs sind oft unsicher. Diese Netzwerke nur mit einer zusätzlichen Sicherheitsmaßnahme wie einem VPN verwenden!

Vertrauenswürdige Netzwerke: Nur mit vertrauenswürdigen Netzwerken verbinden und die automatische Verbindung zu WLAN-Netzwerken deaktivieren.

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

5. Sicherer Umgang mit mobilen Geräten

5. App-Sicherheit

Vertrauenswürdige Quellen: Apps nur aus offiziellen App-Stores (Google Play, Apple App Store) herunterladen, um das Risiko von Malware zu minimieren.

App-Berechtigungen: Prüfe und beschränke die Berechtigungen von Apps auf das notwendige Minimum.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

5. Sicherer Umgang mit mobilen Geräten

6. Backup und Datenverlust

Regelmäßige Backups: Regelmäßig Backups der Daten erstellen, um im Falle eines Geräteverlusts oder einer Datenbeschädigung darauf zugreifen zu können.

Fernlöschung: Die Möglichkeit zur Fernlöschung einrichten, um Daten bei Verlust des Geräts löschen zu können.

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

5. Sicherer Umgang mit mobilen Geräten

7. Sicherer Umgang mit E-Mails und Nachrichten

Phishing-Prävention: Vorsicht bei E-Mails und Nachrichten von unbekannten Absendern. Keine Links anklicken und keine Anhänge öffnen, die verdächtig erscheinen.

Schutz vor Schadsoftware: Eine zuverlässige Anti-Malware-Software installieren, die auch mobile Bedrohungen erkennt.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

5. Sicherer Umgang mit mobilen Geräten

8. Vermeidung von Jailbreaking und Rooting

Keine Manipulation: Das Betriebssystem des Geräts nicht manipulieren (Jailbreaking/Rooting), da dies Sicherheitsfunktionen außer Kraft setzen und das Gerät anfälliger für Angriffe machen kann.

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

5. Sicherer Umgang mit mobilen Geräten

9. Geräteverwaltung

MDM-Lösungen: Unternehmen sollten Mobile Device Management (MDM) verwenden, um Sicherheitsrichtlinien zentral durchzusetzen und Geräte zu überwachen.

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

5. Sicherer Umgang mit mobilen Geräten

10. Schulung und Bewusstsein

Sensibilisierung: Sich selbst und andere Nutzer im sicheren Umgang mit mobilen Geräten schulen, und sie für potenzielle Sicherheitsrisiken sensibilisieren.

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

6. Netzwerksicherheit

Definition von Netzwerksicherheit:

Netzwerksicherheit umfasst alle Maßnahmen und Richtlinien, die dazu dienen, die Integrität, Vertraulichkeit und Verfügbarkeit von Daten und Netzwerkinfrastrukturen zu gewährleisten.

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

6. Netzwerksicherheit

Definition von Netzwerksicherheit:

Dies beinhaltet den Schutz vor unbefugtem Zugriff, Missbrauch, Fehlfunktionen und Datenverlust. Netzwerksicherheit ist ein Teilgebiet der IT-Sicherheit und beschäftigt sich speziell mit der Sicherheit von Kommunikations- und Datennetzwerken.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

6. Netzwerksicherheit

Bedeutung der Netzwerksicherheit in Unternehmen und Organisationen

In einer zunehmend digitalisierten Welt, in der Unternehmen auf vernetzte Systeme angewiesen sind, ist Netzwerksicherheit unverzichtbar. Sie schützt vor Datenverlusten, Diebstahl geistigen Eigentums, finanziellen Schäden und Rufschädigung. Sicherheitsverletzungen können zu Betriebsunterbrechungen führen, die nicht nur finanzielle Verluste, sondern auch langfristige Schäden für das Vertrauen von Kunden und Partnern verursachen.

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

6. Netzwerksicherheit

Überblick über aktuelle Bedrohungslage und Cyberangriffe:

Cyberbedrohungen entwickeln sich ständig weiter, wobei Cyberkriminelle immer raffiniertere Techniken einsetzen. Zu den aktuellen Bedrohungen gehören gezielte Angriffe auf spezifische Organisationen (Advanced Persistent Threats, APTs), Ransomware, die Systeme verschlüsselt und Lösegeld fordert, sowie Angriffe auf Cloud-Infrastrukturen und IoT-Geräte. Zudem sind Angriffe auf kritische Infrastrukturen und nationale Sicherheitsinteressen vermehrt in den Fokus gerückt.

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

6. Netzwerksicherheit

Grundlegende Konzepte der Netzwerksicherheit

Unterschied zwischen internen und externen Netzwerken:

Interne Netzwerke sind Netzwerke innerhalb einer Organisation, die typischerweise geschützt sind und auf vertrauenswürdigen Geräten laufen.

Externe Netzwerke umfassen das Internet oder andere Netzwerke außerhalb der Organisation, die als unsicher gelten. Das Ziel ist, interne Netzwerke vor externen Bedrohungen zu schützen.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

6. Netzwerksicherheit

Grundlegende Konzepte der Netzwerksicherheit

- Perimeter-Sicherheit (z.B. Firewalls)
- Netzwerksegmentierung und –trennung
- VPNs (Virtual Private Networks)

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

6. Netzwerksicherheit
Schutzmechanismen u. Sicherheitsmaßnahmen

- Firewalls: Arten (Hardware, Software, Cloud-basiert), Funktion und Konfiguration
- Intrusion Detection und Prevention Systeme (IDS/IPS)
- Verschlüsselung: VPNs, SSL/TLS, IPsec
- Antivirus- und Antimalware-Software
- Zugriffskontrollen und Authentifizierungsmethoden: Zwei-Faktor-Authentifizierung (2FA), Single Sign-On (SSO)
- Sicherheitsrichtlinien und regelmäßige Audits

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

6. Netzwerksicherheit

Best Practices zur Netzwerksicherheit

Netzwerksegmentierung: Durch die Trennung kritischer Systeme von weniger sensiblen Netzwerken wird die Ausbreitung von Bedrohungen eingeschränkt und der Schaden bei einem Angriff minimiert.

Regelmäßige Updates und Patches: Systeme, Anwendungen und Geräte sollten regelmäßig aktualisiert werden, um bekannte Schwachstellen zu schließen und gegen neue Bedrohungen geschützt zu sein.

Protokollierung und Überwachung: Die Überwachung von Netzwerkaktivitäten und die Protokollierung von Ereignissen helfen, unbefugte Aktivitäten schnell zu erkennen und darauf zu reagieren.

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

6. Netzwerksicherheit

Best Practices zur Netzwerksicherheit

Sicherheitsbewusstsein schulen: Mitarbeiter sollten regelmäßig geschult werden, um Sicherheitsbedrohungen zu erkennen und geeignete Maßnahmen zu ergreifen. Sicherheitsübungen und Phishing-Tests können helfen, das Bewusstsein zu schärfen.

Notfallpläne und Reaktionsstrategien: Ein Incident Response Plan legt fest, wie auf Sicherheitsvorfälle reagiert wird, um Schäden zu minimieren. Business Continuity Planning stellt sicher, dass kritische Geschäftsprozesse auch im Falle eines Ausfalls fortgeführt werden können.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

7. Datensicherung und Wiederherstellung

Datensicherung und Wiederherstellung sind wesentliche Aspekte der Datensicherheit. Sie dienen dazu, Daten vor Verlust, Beschädigung und unbefugtem Zugriff zu schützen und deren Integrität und Verfügbarkeit zu gewährleisten.

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

7. Datensicherung und Wiederherstellung

Datensicherung (Backup)

Regelmäßigkeit: Regelmäßige Datensicherungen sind entscheidend. Die Häufigkeit hängt von der Bedeutung der Daten und der Veränderungsrate ab. Tägliche Backups sind oft ideal, insbesondere für kritische Daten.

Versionierung: Es sollten mehrere Versionen der Backups erstellt werden, um zu unterschiedlichen Zeitpunkten gespeicherte Daten wiederherstellen zu können. Dies schützt vor Datenverlust durch Fehler, Malware oder Ransomware-Angriffe, die Daten beschädigen oder verschlüsseln.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

7. Datensicherung und Wiederherstellung

Datensicherung (Backup)

Speicherort: Backups sollten nicht nur lokal, sondern auch an einem externen Standort gespeichert werden. Cloud-Backups bieten eine zusätzliche Sicherheitsebene, da sie vor physischen Bedrohungen wie Feuer oder Überschwemmungen schützen.

Verschlüsselung: Um die Datensicherheit zu gewährleisten, sollten Backups verschlüsselt werden. Dies verhindert, dass unbefugte Personen im Falle eines Diebstahls oder unbefugten Zugriffs auf die Backup-Medien auf die Daten zugreifen können.

3-2-1 Methode!

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

7. Datensicherung und Wiederherstellung

Datensicherung (Backup)

Integrität: Regelmäßige Überprüfungen der Backups sind notwendig, um sicherzustellen, dass sie intakt und vollständig sind. Eine beschädigte Sicherung kann bei einem Datenverlust unbrauchbar sein.

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

Mittelstand-Digital

7. Datensicherung und Wiederherstellung

Datenwiederherstellung (Recovery)

Testen der Wiederherstellungsprozesse: Es ist entscheidend, die Wiederherstellungsprozesse regelmäßig zu testen, um sicherzustellen, dass die Daten im Ernstfall schnell und vollständig wiederhergestellt werden können. Dies reduziert das Risiko von Ausfallzeiten und Datenverlusten.

Notfallwiederherstellung: Unternehmen sollten einen Notfallwiederherstellungsplan (Disaster Recovery Plan) haben, der klar definiert, wie bei einem Datenverlust vorzugehen ist. Der Plan sollte sowohl technische als auch organisatorische Maßnahmen umfassen.

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

7. Datensicherung und Wiederherstellung

Datenwiederherstellung (Recovery)

Zeitpunkt der Wiederherstellung: Bei der Planung von Backups und der Wiederherstellung ist der Recovery Time Objective (RTO) und der Recovery Point Objective (RPO) zu berücksichtigen. Diese bestimmen, wie lange die Wiederherstellung dauern darf und bis zu welchem Zeitpunkt Daten wiederhergestellt werden sollen.

Zugriffskontrollen: Der Zugriff auf Backup- und Wiederherstellungsdaten sollte streng kontrolliert und auf autorisierte Personen beschränkt sein. Dies minimiert das Risiko von Datenlecks und Missbrauch.

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

7. Datensicherung und Wiederherstellung

Datenwiederherstellung (Recovery)

Zugriffskontrollen: Der Zugriff auf Backup- und Wiederherstellungsdaten sollte streng kontrolliert und auf autorisierte Personen beschränkt sein. Dies minimiert das Risiko von Datenlecks und Missbrauch.

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

7. Datensicherung und Wiederherstellung

Compliance-Anforderungen

Auditierbarkeit: Backups sollten so durchgeführt werden, dass sie auditierbar sind. Das bedeutet, dass nachgewiesen werden kann, wann und wie Daten gesichert und wiederhergestellt wurden. Dies ist oft eine Anforderung in regulierten Branchen.

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

7. Datensicherung und Wiederherstellung

Schutz vor Malware und Ransomware

Isolierung der Backups: Backups sollten isoliert von den Primärsystemen aufbewahrt werden, um sie vor Malware oder Ransomware zu schützen, die die Primärdaten verschlüsseln oder zerstören könnten.

Schnelle Wiederherstellung: Im Fall eines Ransomware-Angriffs sollte der Fokus auf einer schnellen und vollständigen Wiederherstellung liegen, um Betriebsunterbrechungen zu minimieren.

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

7. Datensicherung und Wiederherstellung

Datensicherung und Wiederherstellung sind entscheidende Maßnahmen, um die Sicherheit und Verfügbarkeit von Daten zu gewährleisten. Sie müssen sorgfältig geplant, regelmäßig durchgeführt und streng überwacht werden, um den Schutz vor Datenverlust und unbefugtem Zugriff zu maximieren. Durch die Implementierung einer soliden Backup- und Wiederherstellungsstrategie kann ein Unternehmen sicherstellen, dass es gegen die meisten Bedrohungen gut gerüstet ist.

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

8. Compliance und rechtliche Aspekte

Was ist Compliance?

Compliance bezeichnet die Einhaltung von Gesetzen, Vorschriften, Richtlinien und Standards, die für eine Organisation relevant sind. Im Kontext der Netzwerksicherheit bezieht sich Compliance auf Maßnahmen, die sicherstellen, dass Sicherheitspraktiken und -protokolle den gesetzlichen und regulatorischen Anforderungen entsprechen.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

8. Compliance und rechtliche Aspekte

Wichtige gesetzliche Regelungen und Standards

DSGVO (Datenschutz-Grundverordnung)

Geltungsbereich: Die DSGVO gilt für alle Unternehmen, die personenbezogene Daten von EU-Bürgern verarbeiten, unabhängig davon, wo das Unternehmen seinen Sitz hat.

Anforderungen: Die DSGVO fordert, dass Unternehmen geeignete technische und organisatorische Maßnahmen ergreifen, um den Schutz personenbezogener Daten zu gewährleisten. Dazu gehören Datensicherheitsmaßnahmen, Meldung von Datenschutzverletzungen, Datenschutz-Folgenabschätzungen (DPIA) und die Ernennung eines Datenschutzbeauftragten.

Strafen bei Verstößen: Geldbußen können bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes betragen, je nachdem, welcher Betrag höher ist.

Bundesministerium für Wirtschaft und Klimaschutz
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

8. Compliance und rechtliche Aspekte

Wichtige gesetzliche Regelungen und Standards

BSI-Gesetz und IT-Sicherheitsgesetz (Deutschland)

Geltungsbereich: Unternehmen, die als kritische Infrastrukturen (KRITIS) gelten, sind verpflichtet, die IT-Sicherheit ihrer Systeme zu gewährleisten und Sicherheitsvorfälle zu melden.

Anforderungen: Einführung von IT-Sicherheitsmaßnahmen, Umsetzung eines IT-Sicherheitsmanagementsystems (ISMS), regelmäßige Sicherheitsüberprüfungen und Meldung von Sicherheitsvorfällen an das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

8. Compliance und rechtliche Aspekte
Wichtige gesetzliche Regelungen und Standards

ISO/IEC 27001

Geltungsbereich: Ein international anerkannter Standard für Informationssicherheitsmanagementsysteme (ISMS).

Anforderungen: Die Norm legt Anforderungen an die Einführung, Umsetzung, Aufrechterhaltung und kontinuierliche Verbesserung eines ISMS fest. Dazu gehört die Durchführung von Risikobewertungen, Sicherheitsrichtlinien, Schulung von Mitarbeitern und regelmäßige Audits.

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

8. Compliance und rechtliche Aspekte
Rollen und Verantwortlichkeiten

Datenschutzbeauftragter (DSB): Verantwortlich für die Überwachung der Einhaltung der Datenschutzgesetze, Durchführung von Datenschutz-Folgenabschätzungen und Schulungen.

Chief Information Security Officer (CISO): Verantwortlich für die Entwicklung und Umsetzung der Informationssicherheitsstrategie und die Einhaltung der Sicherheitsrichtlinien.

Mitarbeiter: Alle Mitarbeiter sind verpflichtet, die Sicherheitsrichtlinien und Best Practices einzuhalten und Verdachtsfälle von Sicherheitsverstößen zu melden.

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

8. Compliance und rechtliche Aspekte

Best Practices zur Einhaltung von Compliance und rechtlichen Anforderungen

Risikobewertung und Management: Regelmäßige Risikobewertungen durchführen, um potenzielle Sicherheitslücken zu identifizieren und entsprechende Maßnahmen zu ergreifen**.**

Schulung und Sensibilisierung: Regelmäßige Schulungen für Mitarbeiter über Datenschutz und Sicherheitsrichtlinien, einschließlich des richtigen Umgangs mit Daten und der Erkennung von Phishing-Versuchen.

Zugriffskontrolle: Implementierung von Rollen-basiertem Zugriff (Role-Based Access Control, RBAC) und Multi-Faktor-Authentifizierung (MFA), um den Zugriff auf sensible Daten zu kontrollieren.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

Mittelstand-Digital

8. Compliance und rechtliche Aspekte

Best Practices zur Einhaltung von Compliance und rechtlichen Anforderungen

Überwachung und Protokollierung: Einrichtung von Systemen zur Überwachung und Protokollierung von Netzwerkaktivitäten zur Erkennung von unautorisierten Zugriffen und Anomalien.

Notfall- und Reaktionspläne: Entwicklung und regelmäßige Überprüfung von Plänen für die Reaktion auf Sicherheitsvorfälle, einschließlich der Meldung von Datenschutzverletzungen an die zuständigen Behörden.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

8. Compliance und rechtliche Aspekte

Strafen und Konsequenzen bei Nichteinhaltung

Finanzielle Strafen: Hohe Geldbußen, wie im Fall der DSGVO, können erhebliche finanzielle Belastungen für Unternehmen darstellen.

Reputation: Datenschutzverletzungen und Verstöße gegen Compliance-Vorschriften können den Ruf eines Unternehmens nachhaltig schädigen.

Rechtliche Maßnahmen: Organisationen können mit Klagen und behördlichen Ermittlungen konfrontiert werden.

Betriebsunterbrechungen: Sicherheitsvorfälle können zu Ausfallzeiten und Betriebsunterbrechungen führen, was die Geschäftstätigkeit beeinträchtigen kann.

8. Compliance und rechtliche Aspekte
Abschluss und Zusammenfassung

- ✓ Die Einhaltung von Compliance und rechtlichen Anforderungen ist kein einmaliger Vorgang, sondern ein kontinuierlicher Prozess.
- ✓ Unternehmen sollten proaktiv handeln, indem sie regelmäßige Überprüfungen und Audits durchführen und ihre Sicherheitspraktiken und -richtlinien regelmäßig aktualisieren.
- ✓ Eine Kultur der Sicherheitsbewusstheit und der Verantwortung innerhalb der gesamten Organisation ist entscheidend, um Compliance-Anforderungen zu erfüllen und die Netzwerksicherheit zu gewährleisten.

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

9. Incident Response und Krisenmanagement

Incident Response (IR) ist ein systematischer Ansatz zur Bewältigung von Sicherheitsvorfällen, die die Integrität, Vertraulichkeit oder Verfügbarkeit von Daten gefährden. Der Prozess stellt sicher, dass Bedrohungen schnell identifiziert, eingedämmt und behoben werden, um den Schaden zu minimieren.

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

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Vorbereitung:

Entwicklung und Implementierung von Sicherheitsrichtlinien und -verfahren.

Schulung des Incident-Response-Teams und Durchführung regelmäßiger Sicherheitsübungen.

Etablierung von Kommunikationsplänen und Eskalationsprozessen.

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

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Identifizierung:

Erkennung und Meldung von Sicherheitsvorfällen mithilfe von Monitoring-Tools.

Analyse der Vorfälle, um das Ausmaß und die Auswirkungen zu bestimmen.

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

Mittelstand-Digital

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Eindämmung:

Kurzfristige Maßnahmen zur Begrenzung der Ausbreitung des Vorfalls.

Entscheidung über temporäre Lösungen (z. B. Isolierung betroffener Systeme).

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

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Beseitigung:

Identifizierung und Behebung der Ursache des Vorfalls.

Bereinigung der Systeme von Schadsoftware oder kompromittierten Daten.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Wiederherstellung:

Wiederherstellung der betroffenen Systeme und Services in den Normalbetrieb.

Durchführung von Systemtests, um sicherzustellen, dass die Bedrohung vollständig beseitigt ist.

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

9. Incident Response und Krisenmanagement

Phasen des Incident Response

Lessons Learned:

Nachbesprechung des Vorfalls zur Analyse, was gut lief und was verbessert werden kann.

Aktualisierung der Sicherheitsrichtlinien und des Incident-Response-Plans basierend auf den Erkenntnissen.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Krisenmanagement geht über die reine Incident Response hinaus und konzentriert sich auf die strategische Bewältigung von schwerwiegenden und oft unerwarteten Vorfällen, die das gesamte Unternehmen betreffen können.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Krisenplan:

Ein detaillierter Plan, der Rollen, Verantwortlichkeiten und Prozesse definiert, um auf eine Krise zu reagieren. Der Plan sollte auch Kommunikationsstrategien beinhalten, um Informationen intern und extern zu teilen.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Krisenteam:

Zusammensetzung eines interdisziplinären Teams, das für die Bewältigung der Krise verantwortlich ist. Klar definierte Rollen und Verantwortlichkeiten, einschließlich eines Krisenmanagers.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Krisenkommunikation:

Entwicklung eines Kommunikationsplans für den internen und externen Austausch von Informationen.

Transparente und zeitnahe Kommunikation mit Stakeholdern (Mitarbeiter, Kunden, Partner, Regulierungsbehörden), um das Vertrauen zu erhalten und die Auswirkungen der Krise zu managen.

Die Kommunikation sollte koordiniert und konsistent sein.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Szenarioanalyse und Planung:

Identifizierung potenzieller Krisenszenarien (z. B. Datenlecks, Ransomware-Angriffe).

Entwicklung von Plänen und Notfallmaßnahmen für jedes Szenario.

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

9. Incident Response und Krisenmanagement

Krisenmanagement

Übungen und Simulationen:

Regelmäßige Durchführung von Krisensimulationen, um die Reaktionsfähigkeit des Unternehmens zu testen.

Bewertung und Anpassung der Krisenpläne basierend auf den Übungsergebnissen

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

9. Incident Response und Krisenmanagement

Verbindung zwischen Incident Response und Krisenmanagement

Incident Response ist ein integraler Bestandteil des Krisenmanagements.

Während Incident Response sich auf die technische Reaktion und Eindämmung konzentriert, bezieht sich Krisenmanagement auf die strategische Bewältigung der Auswirkungen eines Vorfalls auf die gesamte Organisation.

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

9. Incident Response und Krisenmanagement

Verbindung zwischen Incident Response und Krisenmanagement

Nicht jeder Sicherheitsvorfall führt zu einer Krise. Jedoch können gravierende Vorfälle eskalieren und das Krisenmanagement erfordern, insbesondere wenn sie die Geschäftskontinuität oder das öffentliche Image erheblich gefährden.

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

10. Mitarbeitertraining

Mitarbeitertraining bezüglich Datensicherheit ist ein zentraler Bestandteil jeder umfassenden Sicherheitsstrategie. Menschen sind oft das schwächste Glied in der Sicherheitskette, da sie Ziel von Social Engineering, Phishing und anderen Arten von Angriffen werden können. Durch regelmäßige Schulungen können Mitarbeiter zu einer wichtigen Verteidigungslinie gegen Datenverluste und Sicherheitsverletzungen werden.

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

10. Mitarbeitertraining

Beispiel für Themen und Informationen, die in einem Mitarbeitertraining zur Datensicherheit behandelt werden sollten:

✓ **Einführung in Datensicherheit**

Definition: Was ist Datensicherheit und warum ist sie wichtig?

Bedeutung: Diskussion über die Bedeutung von Datensicherheit für das Unternehmen und die persönlichen Auswirkungen von Sicherheitsverstößen (z.B. Identitätsdiebstahl, finanzielle Schäden).

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

10. Mitarbeitertraining

✓ **Verständnis für Bedrohungen**

Phishing: Erläuterung, was Phishing ist, wie solche Angriffe typischerweise aussehen und wie man sie erkennen kann.

Malware und Ransomware: Wie diese Arten von Schadsoftware in Systeme gelangen können und welche Schäden sie verursachen. Beispiele für bekannte Angriffe (z.B. WannaCry).

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

10. Mitarbeitertraining

✓ **Verständnis für Bedrohungen**

Social Engineering: Wie Angreifer versuchen, durch Täuschung und Manipulation an vertrauliche Informationen zu gelangen. Beispiele für gängige Methoden (z.B. CEO Fraud, Tailgating).

Insider-Bedrohungen: Erklärung, dass auch eigene Mitarbeiter versehentlich oder absichtlich Daten kompromittieren können.

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

Mittelstand-Digital

10. Mitarbeitertraining

✓ Sichere Passwortpraktiken

Erstellung sicherer Passwörter: Hinweise zur Erstellung von starken, einzigartigen Passwörtern (z.B. Nutzung von Passphrasen, Kombination aus Buchstaben, Zahlen und Sonderzeichen).

Passwort-Management: Empfehlung von Passwort-Managern zur Verwaltung und sicheren Speicherung von Passwörtern.

Regelmäßige Passwortänderungen: Erklärung, warum und wie oft Passwörter geändert werden sollten.

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

Mittelstand-Digital

10. Mitarbeitertraining

✓ **Sicherer Umgang mit Unternehmensdaten**

Klassifizierung von Daten (z. B. öffentlich, vertraulich, streng vertraulich)

Sichere Speicherung und Übertragung sensibler Daten

Nutzung von Verschlüsselungstechniken für E-Mails und Dateien

Maßnahmen zur Sicherung mobiler Geräte (z. B. Laptops, Smartphones)

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

10. Mitarbeitertraining

✓ **Nutzung von Netzwerken und Geräten**

Risiken von öffentlichem WLAN und wie man sich schützt (z. B. Nutzung von VPNs)

Sicherer Umgang mit externen Speichermedien (z. B. USB-Sticks)

Richtige Konfiguration und Nutzung von privaten Geräten für Unternehmenszwecke (BYOD-Richtlinien)

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

Mittelstand-Digital

10. Mitarbeitertraining

✓ Reaktion auf Sicherheitsvorfälle

Identifizierung eines Sicherheitsvorfalls

Interne Protokolle zur Meldung und Reaktion

Wichtige Ansprechpartner im Unternehmen bei Sicherheitsvorfällen

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

Mittelstand-Digital

10. Mitarbeitertraining
Best Practices für effektive Datensicherheitsschulungen

Regelmäßige Auffrischungen: Datensicherheitsbedrohungen ändern sich ständig, daher sollten Schulungen regelmäßig aktualisiert und wiederholt werden.

Anpassung an die Zielgruppe: Schulungsinhalte sollten auf die spezifischen Rollen und Verantwortlichkeiten der Mitarbeiter abgestimmt sein.

Einbindung des Managements: Führungskräfte sollten die Schulungen unterstützen und selbst daran teilnehmen, um ein gutes Vorbild zu geben.

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

10. Mitarbeitertraining
Best Practices für effektive Datensicherheitsschulungen

Feedback und kontinuierliche Verbesserung: Nach den Schulungen sollte Feedback eingeholt und genutzt werden, um zukünftige Schulungen zu verbessern.

Messung des Erfolgs: Überwachung und Bewertung der Wirksamkeit von Schulungsprogrammen durch Tests und Überprüfung des Bewusstseins und Verhaltens der Mitarbeiter.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

10. Mitarbeitertraining

Fazit

Ein effektives Mitarbeitertraining zur Datensicherheit ist entscheidend für den Schutz von Unternehmensdaten und den Aufbau einer Sicherheitskultur im Unternehmen. Es hilft nicht nur, das Risiko von Sicherheitsverletzungen zu minimieren, sondern stärkt auch das Vertrauen der Kunden und Partner in die Sicherheitskompetenz des Unternehmens. Durch kontinuierliche Schulung und Sensibilisierung können Mitarbeiter dazu befähigt werden, eine aktive Rolle in der Cybersicherheit ihres Unternehmens zu spielen.

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

11. Fallstudien und Praxisbeispiele

Target-Datenleck (2013)

Vorfall: Cyberkriminelle drangen in das Zahlungssystem von Target ein und erbeuteten Kreditkartendaten von etwa 40 Millionen Kunden.

Ursache: Der Angriff begann mit einem Phishing-Angriff auf einen Drittanbieter von Target. Ein Mangel an segmentierten Netzwerken ermöglichte es den Angreifern, von einem Zugangspunkt aus auf sensible Systeme zuzugreifen.

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

11. Fallstudien und Praxisbeispiele

Target-Datenleck (2013)

Folgen: Target musste erhebliche Kosten tragen, darunter Entschädigungen an Kunden und die Verbesserung der Sicherheitsinfrastruktur. Der Vorfall führte auch zu Veränderungen im Top-Management.

Lehren: Es ist wichtig, die Sicherheitspraktiken von Drittanbietern zu überwachen und sicherzustellen, dass Netzwerke segmentiert sind, um die Ausbreitung von Angriffen zu verhindern.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

11. Fallstudien und Praxisbeispiele

Sony Pictures Hack (2014)

Vorfall: Eine Gruppe, die sich „Guardians of Peace“ nannte, drang in das Netzwerk von Sony Pictures ein und stahl eine enorme Menge an vertraulichen Daten, darunter E-Mails, Finanzdaten und unveröffentlichte Filme.

Ursache: Der Angriff wurde vermutlich durch Spear-Phishing oder eine gezielte Infektion von Systemen mit Schadsoftware ermöglicht.

Die in dieser Präsentation enthaltenen Angaben beziehen sich grundsätzlich auf alle Geschlechter (m/w/d). Zur besseren Lesbarkeit wurde im Text in der Regel die männliche Form verwendet. Wir bitten um die Wahrung unserer Fabrikations-, Betriebs- und Geschäftsgeheimnisse gem. § 111 GWB.

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

11. Fallstudien und Praxisbeispiele

Sony Pictures Hack (2014)

Folgen: Der Vorfall führte zu erheblichen finanziellen Verlusten, einer Rufschädigung und internen Umstrukturierungen.

Lehren: Unternehmen sollten sich gegen zielgerichtete Phishing-Angriffe wappnen und ihre Systeme gegen Malware absichern. Eine regelmäßige Schulung der Mitarbeiter in Bezug auf Sicherheitsbewusstsein ist ebenfalls wichtig.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

11. Fallstudien und Praxisbeispiele

NSO Group Pegasus-Spyware (2021)

Vorfall: Die israelische Firma NSO Group entwickelte die Spyware "Pegasus", die verwendet wurde, um Mobiltelefone hochrangiger Personen weltweit auszuspionieren.

Ursache: Pegasus nutzte Zero-Day-Schwachstellen in Mobilgeräten, um auf persönliche Daten zuzugreifen, ohne dass die Opfer davon wussten.

Gefördert durch: Bundesministerium für Wirtschaft und Klimaschutz aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

11. Fallstudien und Praxisbeispiele

NSO Group Pegasus-Spyware (2021)

Folgen: Der Skandal führte zu internationalen Kontroversen und Diskussionen über die Regulierung von Überwachungssoftware.

Lehren: Schwachstellenmanagement in mobilen Betriebssystemen ist kritisch. Es zeigt auch die Notwendigkeit einer globalen Diskussion über die ethischen Grenzen von Überwachungstechnologien.

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