IT-RISIKOMANAGEMENT

Das Fundament jedes Cyber Security Konzepts

7. Juni 2023

BDO

VORSTELLUNG

BDO Consulting / Cyber Security

Mario
Neubauer
Senior Manager

+43 664 60 375 - 4253
mario.neubauer@bdo.at

bdo.at/cyber

BEREICH: CONSULTING

Innovation, Transformation und Sicherheit brauchen die besten Köpfe - BDO Consulting hat sie.

Wir begegnen komplexen Aufgabenstellungen mit breiten, innovativen Lösungen, state-of-the-art Tools und umfassendem Know-how - von der ersten Analyse bis zur finalen Implementierung, national sowie international.

Denn unser Ziel ist Ihr nachhaltiger Erfolg!

Cyber Security

Nachhaltige Ergebnisverbesserung

Risk & Resilience

Digital Services

Information Technology

Management Consulting

Förderung und Forschung

WER WIR SIND

BDO AUSTRIA

Großartiges Unternehmertum verdient besondere Aufmerksamkeit!

Nur wer zuhört und versteht, kann Sie auch umfassend betreuen. Darum ist BDO Ihr verlässlicher Wegbegleiter. Zusammen stellen wir die Weichen für Ihr Projekt und finden passende Lösungen - damit Sie sicher ins Ziel kommen.

Für Ihre Strategie setzen wir alle Hebel in Bewegung: Je nach Aufgabenstellung stellen wir das optimale Team für Sie zusammen.

Das macht uns zu BDO.
Und uns gemeinsam great.

OFFICES

WIEN, GRAZ, LINZ, SALZBURG, KLAGENFURT, DORNBIRN, JUDENBURG, WOLFSBERG, EISENSTADT, BRUCK/LEITHA, OBERWART

SERVICE AREAS

ACCOUNTING, ASSURANCE, CONSULTING, CORPORATE FINANCE, PEOPLE & ORGANISATION, TAX

KUND:INNEN
13.300+

MITARBEITER:INNEN
1.000+

PARTNER:INNEN
60

STANDORTE
in ganz Österreich

UMSATZ 2021/22
EUR 113,5 MIO.

GRÜNDUNG
1976

Stand: Dezember 2022

WER WIR SIND

BDO INTERNATIONAL

Sie möchten Ihr Potenzial auch international ausschöpfen?

Wenn Sie Ihr Weg auf der Suche nach Greatness in die unterschiedlichsten Länder führt, sind Sie mit uns ideal unterwegs. Das BDO Netzwerk heißt Sie weltweit willkommen und begleitet Sie über alle Ländergrenzen hinweg zum Ziel.

Wir sehen Ihren großartigen Plänen mit Freude entgegen!

NETZWERK

Die BDO Gruppe Österreich ist Teil des weltweit tätigen BDO Netzwerks von Wirtschaftsprüfer:innen, Steuer- und Unternehmensberater:innen.

MITARBEITER:INNEN	LÄNDER	BÜROS	GRÜNDUNG	UMSATZ 2021/22
111.300+	160+	1.803	1963	USD 12,8 MRD.

Stand: Dezember 2022

Accounting

Konzentrieren Sie sich auf Ihre Kernkompetenzen. Die Abwicklung Ihrer Finanzprozesse ist bei uns in guten Händen und liefert die Basis für Ihre unternehmerischen Entscheidungen.

Assurance

Vertrauen und Mehrwert sind die Basis unserer Zusammenarbeit. Im Fokus stehen dabei stets persönliche Betreuung sowie höchste internationale Prüfungs- und Qualitätsstandards.

Consulting

Bringen Sie Ihr Unternehmen nachhaltig in Topform! Ein versiertes Team sorgt mit einer breiten Palette an Tools und Know-how für individuelle und innovative Lösungen.

Corporate Finance

Fundierte Grundlagen stellen die Basis unternehmerischer Entscheidungen dar. Mit dem richtigen Partner stellen Sie Ihr Unternehmen für die Zukunft optimal auf.

People & Organisation

Der Mensch ist der entscheidende Erfolgsfaktor eines jeden Unternehmens. Vertrauen Sie in einer Welt des Arbeitsumbruchs auf einen starken Wegbegleiter.

Tax

Sie möchten auf dem Markt erfolgreich sein? Mit einem zukunftsorientierten Partner an Ihrer Seite stehen Ihrem Erfolg die Türen offen.

EINE RUNDE SACHE

UNSERE EXPERTISE FÜR IHR UNTERNEHMEN

BDO AUSTRIA - KOMMUNALCENTER

Ihr lokaler Partner im globalen Netzwerk

DER BEGLEITER FÜR KOMMUNEN AUF DEM WEG…

… zur wirtschaftlich abgesicherten Gemeinde mit nachhaltigem Zukunftspotential

MITARBEITER:INNEN IM KOMMUNALCENTER	GEMEINDEN	STANDORTE	GRÜNDUNG
30	500+	in ganz Österreich	1976

TEAM

BDO KOMMUNALCENTER

Andreas Schlögl
Partner

Günter Toth
Partner

Peter Pilz
Partner

Petra Simonis-Ehtreiber
Director

Silke Pöll
Senior Managerin

Jasmin Böhm ● Andrea Felber ● Silke Halper ● Rebecca Jandrisits-Radakovits

Tamara Kacsits ● Merle Carina Klein ● Michaela Loske-Vittorelli ● Manfred Mertel

Claudia Ostermann ● Klaudia Pichler ● Dietmar Pilz ● Manuel Prehm ● Verena Putz

Oliver Rosenfelder ● Marion Wingelhofer ● Andrea Wukits

AGENDA

- Aktuelle Bedrohungen
- Aktuelle Gesetzeslage
  - Netz- und Informationssicherheitsrichtlinie 2 (NIS2)
- IT-Risikoanalyse
- Beispiel IT-Risikoanalyse

AKTUELLE BEDROHUNGEN

CYBER SECURITY RISIKEN

Cyber Crime und seine Auswirkungen

REPUTATIONSVERLUST

Website Defacement
Fake News
Datenlecks

DATENDIEBSTAHL

Hacking von Webseiten und IT-Netzwerken über Schwachstellen

ERPRESSUNG

Denial-of-Service Angriffe
Ransomware

AUSNUTZUNG VON RESSOURCEN

Crypto-Mining
Botnetze

SPIONAGE

Social Engineering
Phishing

BETRUG

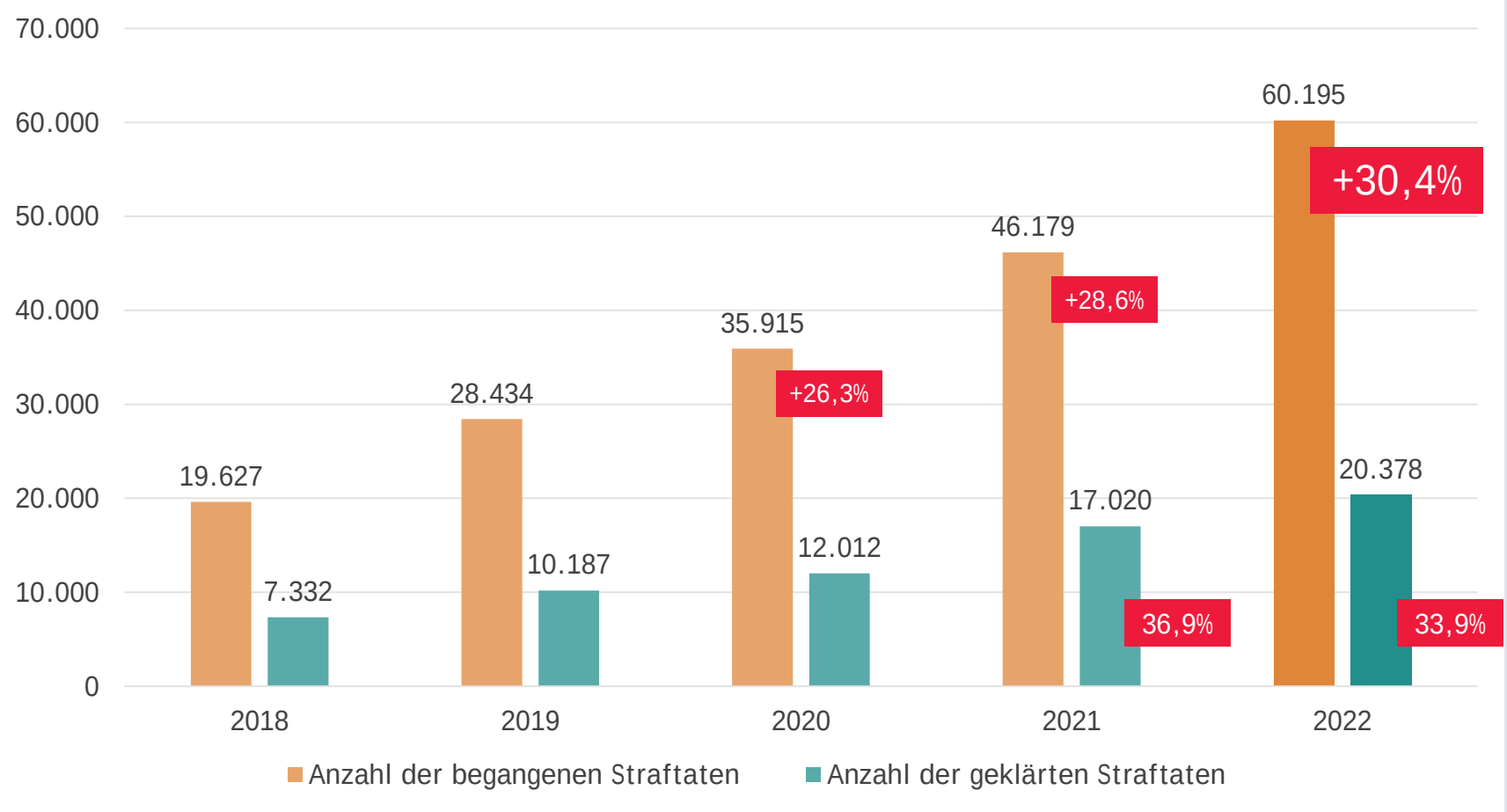
CEO - Fraud
Fake President Angriffe

SABOTAGE

Lahmlegen des Unternehmens
Ransomware

CYBER CRIME IN ÖSTERREICH

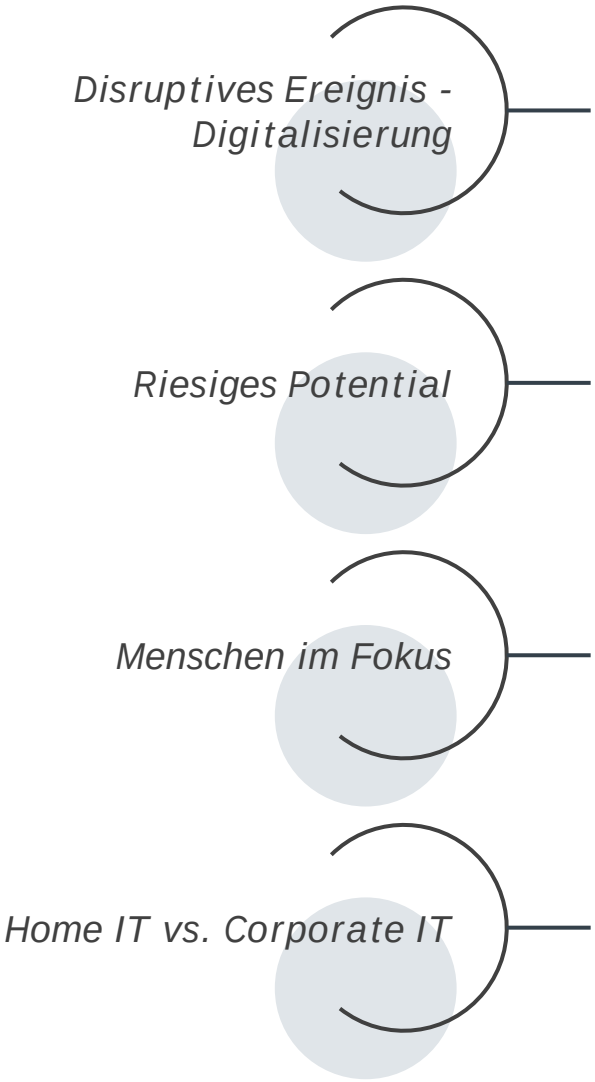
Straftaten vs. geklärte Straftaten - Report 2022



https://bundeskriminalamt.at/306/files/Cybecrime_2022_V20230517_webBF.pdf

COVID-19 - KATALYSATOR FÜR CYBERKRIMINALITÄT

Cyber Crime - IT-Kriminalität als weltweit hochprofitables Geschäft



Disruptives Ereignis - Digitalisierung

- Die COVID-19 Pandemie war für viele Unternehmen ein disruptives Ereignis. In kürzester Zeit mussten Digitalisierungsthemen, die eigentlich gute Planung benötigen, eingerichtet werden.

Riesiges Potential

- Die Cyberkriminalität ist zu Beginn der Pandemie stark angestiegen.
- Unzählige Unternehmen öffneten ihre Firewall für Remote-Services.
- Im Zuge der raschen Umstellung wurde IT-Security hinten angestellt.

Menschen im Fokus

- Besonders nicht-technische Angriffsvektoren wie Spam-E-Mails, Ransomware und (Spear-) Phishing stehen im Vordergrund.
- Die Gutgläubigkeit der Menschen wird ausgenutzt!

Home IT vs. Corporate IT

- Die private Infrastruktur steht nicht unter dem Schutz der Corporate IT. Das Sicherheitsniveau ist häufig schlecht.
- Risiko: Geräte werden auch von anderen Personen genutzt.

CYBER CRIME AS A SERVICE

Dienstleistungen / Schadsoftware zu günstigen Preisen

Was ist CaaS

- Hackergruppen verkaufen ihre Produkte an andere (weniger versierte) Hacker
- Vertrieb über Foren im Untergrund (Darknet)
- Reputationsbasiert - man muss sich in den Foren erst beweisen
- Bezahlung über Crypto-Währungen

Dienstleistungen

- Distributed Denial of Service (DDoS)
- Ransomware as a Service
- Access as a Service
- Verkauf von Schwachstellen und Exploits

Umsatzmodelle

- Monatsabonnement
- Gewinnbeteiligung (in der Regel 20-30 %)
- Einmaliger Lizenzkauf
- Aufwandsbasiert (z.B. bei DDoS)

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

TAUSENDE BETROFFEN

Land Kärnten nach Hackerangriff im Notbetrieb

Attacke wurde Dienstag bemerkt. Komplettes IT-System musste heruntergefahren werden. Dass Daten gestohlen worden sind, sei unwahrscheinlich, könne aber nicht ausgeschlossen werden.

Was ist passiert?

- Am 24.5.2022 fand eine Cyber-Attacke durch die international gesuchte Hacker-Gruppe „Black Cat" statt. Hierbei wurde begonnen die Daten des Landes zu verschlüsseln; aus derzeitiger Sicht wurden teilweise Daten kopiert. Aus Sicherheitsgründen mussten Teile des Landes IT-Netzes und damit verbundene Anwendungen still gelegt werden. Das Amt der Kärntner Landesregierung war kurzfristig per E-Mail und teilweise per Telefon (Internettelefonie) nicht erreichbar.

Digital Life

Hackerangriff auf Kärnten: Angreifer nutzten Phishing-Mail

Die gesamte Telefonanlage ist ausgefallen, das Mailsystem funktioniert auch nicht. Rund 3.900 Mitarbeiter und etwa 3.000 PC-Anschlüsse sind betroffen

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

06.09.2022, 21:51

Hackerangriff auf Steirer-Gemeinde – Lösegeld gefordert

Am Wochenende wurden Mitarbeiter der Stadtgemeinde Feldbach (ST) auf einen Cyber-Angriff aufmerksam. Die Hacker fordern Lösegeld in Bitcoin.

Mit einem Verschlüsselungstrojaner haben Hacker die Stadtgemeinde Feldbach angegriffen. Bis zu 10 Terabyte an Daten auf dem Verwaltungsserver könnten betroffen sein.

ERFOLGREICHE ANGRIFFE AUS DER VERGANGENHEIT

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

DATEN GESTOHLEN

Hacker-Angriff auch auf Weiz: „Wir hatten Glück“

Hacker haben die Verwaltung der Stadtgemeinde Feldbach lahmgelegt und fordern Lösegeld. Vor zwei Jahren war Weiz mit einer ähnlichen Cyber-Attacke konfrontiert - und kam glimpflich davon.

Nichts ist passiert. Und so kann Eggenreich mittlerweile gelassener über den Vorfall im Mai 2020 sprechen. Damals war die Stadt Weiz Opfer eines Angriffs von Hackern. Gestohlen wurden insgesamt 27 Gigabyte an Daten von einem alten Laufwerk aus dem Jahr 2018. Die Diebe drohten damit, die Beute im sogenannten Darknet, einem abgeschotteten Sammelplatz von Kriminellen im Internet, zu veröffentlichen - und sie wollten eine hohe Summe in der Kryptowährung Bitcoin.

Damals war die Stadt Weiz Opfer eines Angriffs von Hackern. Gestohlen wurden insgesamt 27 Gigabyte an Daten von einem alten Laufwerk aus dem Jahr 2018.

RISIKO FÜR GEMEINDEN UND KLEINERE BETRIEBE HOCH!

Cybercrime- IT-Kriminalität als weltweit hochprofitables Geschäft

2023 im Fokus: Gemeinden und kleinere Betriebe

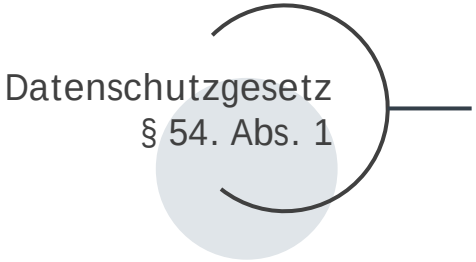
„Derartige Angriffe kommen und gehen in Wellen", erklärt **Otmar Lendl**, Cybersicherheitsexperte beim Computer Emergency Response Team Austria (**CERT.at**). Künftig könnten vermehrt **kleinere Firmen** und Institution ins Visier der Hacker geraten, so Lendl. Sie haben oft nur kleine IT-Abteilungen und deswegen nur eingeschränkt Ressourcen für umfangreiche Schutzmaßnahmen. „Es ist zu erwarten, dass es 2023 verstärkt **Gemeinden** erwischen wird", beschreibt Lendl. Deshalb werden die Erpresser in Österreich auch dieses Jahr viele Betriebe herausfordern, so der Experte.

https://futurezone.at/b2b/ransomware-cybersecurity-2022-2023-bedrohung-it-sicherheit-cert-sophos/402267504

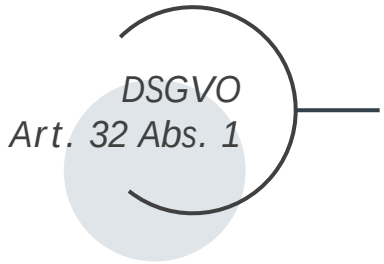
AKTUELLE GESETZESLAGE

DATENSCHUTZGESETZE

DSG & DSGVO



- Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen, unter Berücksichtigung der unterschiedlichen Kategorien gemäß § 37, geeignete technische und organisatorische Maßnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten gemäß § 39.



- Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;

NETZ- UND INFORMATIONSSYSTEMSICHERHEITSGESETZ (NISG)

Bisherige Anforderungen der NIS1

§11 (1) Sicherheitsvorkehrungen gemäß § 17 Abs. 1 NISG, die geeignet sind und den Stand der Technik berücksichtigen sowie zur Gewährleistung der Netz- und Informationssystemsicherheit (§ 3 Z 2 NISG) zu treffen.

Insg. 29 Kontrollen/Anforderungen

Kapitel	Bezeichnung
1	Governance und Risikomanagement
2	Umgang mit Dienstleistern, Lieferanten und Dritten
3	Sicherheitsarchitektur
4	Systemadministration
5	Identitäts- und Zugriffsmanagement
6	Systemwartung und Betrieb
7	Physische Sicherheit
8	Erkennung von Vorfällen
9	Bewältigung von Vorfällen
10	Betriebskontinuität
11	Krisenmanagement

DER WEG ZUR NIS2

Netz- und Informationssystemsicherheitsgesetz (NISG)

EU Richtlinie

- NIS 2 RL: am 16.12.2020 als Teil der neuen EU Cybersicherheitsstrategie von EU-Kommission (DG CONNECT) vorgelegt
  - in Kraft seit 16. Jänner 2023
  - legt Maßnahmen fest, mit welchen ein hohes gemeinsames Sicherheitsniveau von Netz- und Informationssystemen in der EU erreicht werden soll
  - ersetzt die bisherigen Regeln der NIS 1 RL

Nationale Umsetzung

- 21 Monate Umsetzungsfrist für Mitgliedstaaten
  - Anpassung des NISG bis voraussichtlich August 2024
  - Details der nationalen Umsetzungsgesetzgebung derzeit noch offen

NIS2 - BETROFFENE UNTERNEHMEN

Anforderungen aus NIS2

Wesentliche Einrichtungen
(ca. 900)

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Digitale Infrastruktur
- Abwasser
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

Wichtige Einrichtungen
(ca. 2.500)

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie
- Lebensmittel
- verarbeitendes/herstellendes Gewerbe
- Anbieter digitaler Dienste
- Forschung (fakultativ)

NIS2 - BETROFFENE UNTERNEHMEN

Anforderungen aus NIS2

Wesentliche Einrichtungen
(ca. 900)

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Digitale Infrastruktur
- Abwasser
- Verwaltung von IKT-Diensten B2B
- öffentliche Verwaltung
- Weltraum

f) die Einrichtung eine Einrichtung der öffentlichen Verwaltung:

i) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung der Zentralregierung ist oder

ii) von einem Mitgliedstaat gemäß nationalem Recht definierte Einrichtung der öffentlichen Verwaltung auf regionaler Ebene ist, die nach einer risikobasierten Bewertung Dienste erbringt, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Tätigkeiten haben könnte.

(5) Die Mitgliedstaaten können vorsehen, dass diese Richtlinie Anwendung findet auf:

a) Einrichtungen der öffentlichen Verwaltung auf lokaler Ebene;

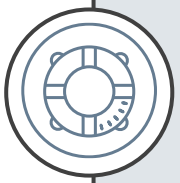
4 HAUPTBEREICHE ZUR UMSETZUNG

Anforderungen aus NIS2

Artikel 20

Governance

- Nimmt Leitungsorgane der Einrichtungen in die Verantwortung.
- Haftungsthema! (*„[...] management bodies [...] can be held liable for infringements [...]“* Artikel 20 Abs.1)



Artikel 21

Risikomanagement-maßnahmen

- gefahrenübergreifenden Ansatz / All-Hazards Approach
- Geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen sowie Berücksichtigung des Stands der Technik sowie der Kosten der Umsetzung

Artikel 23

Berichtspflichten

- Es muss das CSIRT unverzüglich über jeden Sicherheitsvorfall unterrichtet werden, wenn der Sicherheitsvorfall erhebliche Auswirkungen auf die Erbringung der Dienste hat.

Artikel 32

Aufsichts- und Durchsetzungs-maßnahmen

- Zuständige Behörden mit Aufsichtsaufgaben, welche die Umsetzung der Maßnahmen (v.a. Artikel 21) überprüfen und Verstöße aufzeigen.

DIE 10 MAßNAHMEN

Risikomanagementmaßnahmen - Artikel 21

Nr	Maßnahmen / Beschreibung
1	Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
2	Bewältigung von Sicherheitsvorfällen;
3	Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
4	Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
5	Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen; (Anm.: Betriebssicherheit)
6	Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
7	grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
8	Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
9	Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
10	Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung. (Anm.: Kommunikationssicherheit)

NR 1 - RISIKOANALYSE UND SICHERHEIT FÜR INFORMATIONSSYSTEME

Risikomanagementmaßnahmen - Artikel 21

Risikomanagement

- Klein starten (Excel) und stetig verbessern!
- Regelmäßige Durchführung (z.B. monatlich)
- Fokus auf die wichtigsten Systeme (BIA)

Das Rad nicht neu erfinden!

- Standards heranziehen:
  - ISO 27001
  - BSI 200-3

Quelle: BSI - https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-IT-Grundschutz/Lektion_7_Risikoanalyse/Lektion_7_node.html

NR 3 - SICHERHEIT DER LIEFERKETTE

Risikomanagementmaßnahmen - Artikel 21

Risikoanalyse durchführen

- Bewertung aller verbundenen Risiken und potenzieller Bedrohungen zu direkten Lieferanten und Diensteanbietern

Anforderungen an Dienstleister definieren

- Festlegung vertraglicher Vereinbarungen
  - Sicherheitsanforderungen, Qualitätssicherungsmaßnahmen, Produktionsprozesse, …

Management der Lieferkette

- Festlegung klarer Prozesse zur Verwaltung der direkten Lieferanten und Diensteanbietern
- Sicherstellung von Sicherheitsstandards

Aktive Überwachung

- Regelmäßige Überwachung der Lieferkettenprozesse
- Aktive Überwachung der Verbindungen
- Überprüfung der Sicherheitsmaßnahmen (Lieferantenaudits)

RISIKOANALYSE

Kenne deine Risiken

ZIELE DER RISIKOANALYSE

Risikoanalyse

Früherkennung

- Erkennung potenzieller Risiken im Frühstadium
- Behebung von Kontrollschwächen
- Minimierung möglicher Folgekosten

Schutz der Assets

- Abwehr potenzieller Bedrohungen
- Effektiver Schutz von Vermögenswerten wie Daten oder Systemen
- Gewährleistung der Geschäftsfortführung

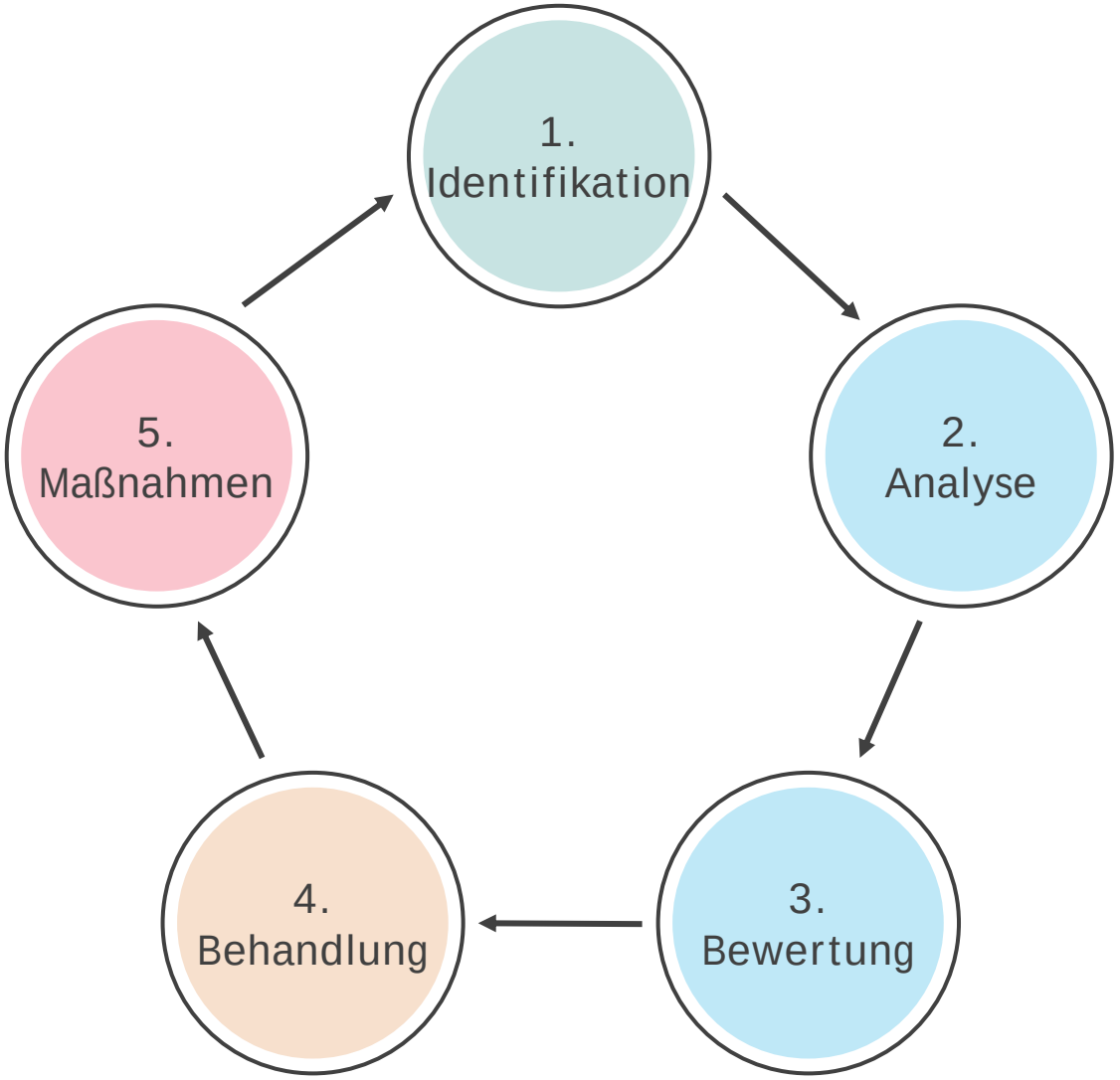
Kostenoptimierung

- Besseres Verständnis der Geschäftsprozesse
- Kosteneinsparungen durch bewussten Einsatz von Firmenressourcen
- Vermeidung von Fehlentscheidungen

DIE RISIKOANALYSE IST DAS FUNDAMENT ALLER (CYBER SECURITY) ENTSCHEIDUNGEN!

RISIKOANALYSE

Wesentliche Schritte einer Risikoanalyse



RISIKOIDENTIFIKATION

Wesentliche Schritte einer Risikoanalyse

Risiko-identifikation

- Ermittlung potenzieller Risiken
  - Vergangene Probleme
  - Analyse aktueller Gefahrentrends
  - Ausgangsbasis bspw. Gefährdungskataloge des BSI (Elementare Gefährdungen[1], IT-Grundschutz-Bausteine[2])
- Ermittlung der Vermögenswerte
- Dokumentation bestehender Maßnahmen
- Vor allem wichtige Systeme / Prozesse betrachten (Hoher Schutzbedarf)

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/Elementare_Gefaehrdungen.html?nn=128562
[2] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html

RISIKOIDENTIFIKATION

Wesentliche Schritte einer Risikoanalyse

Vergangene Vorfälle

- Analyse vergangener Vorfälle
  - Beobachtung der Ursachen und Auswirkungen
  - Schlussfolgerungen für verwendete Assets ziehen

Bedrohungsquellen identifizieren

- Identifizierung von Schwachstellen
  - Vulnerability Assessments, Penetration Tests
- Logdateienanalyse
  - Firewall-, IDS- und IPS-Logs

Branchen- und Markttrends

- Up-to-date über die aktuelle Gefahrenlandschaft
- Schwachstellen in eingesetzten Produkten

Dokumentation

- Dokumentation identifizierter Bedrohungen
  - Detaillierte Beschreibung
  - Kategorisierung nach Art, Ursprung und Schweregrad
  - Priorisierung und Bewertung

BSI GEFÄHRDUNGSKATALOG - RISIKOKATEGORIEN

Beispiel einer Risikoanalyse

- Elementare Gefährdungen
  - z.B. Manipulation von Informationen, Unbefugtes Eindringen in IT-Systeme, etc.
- Höhere Gewalt:
  - z.B. Ausfall von IT-Systemen, Kabelbrand, Datenverlust durch starke Magnetfelder, etc
- Organisatorische Mängel:
  - z.B. Unzureichende Kontrolle der Sicherheitsmaßnahmen, unbefugter Zutritt in schutzbedürftigen Raum, etc.
- Menschliche Fehlhandlungen:
  - z.B. Vertraulichkeits- oder Integritätsverlust von Daten durch Fehlverhalten, Fehlerhafte Nutzung von IT-Systemen, etc.
- Technisches Versagen:
  - z.B. Ausfall der Stromversorgung, Verlust gespeicherter Daten, Veralten von Kryptoverfahren, etc.
- Vorsätzliche Handlungen
  - z.B. Manipulation oder Zerstörung von Geräten oder Zubehör, Unbefugtes Eindringen in ein Gebäude, Diebstahl, etc.

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse

Risiko-bewertung

- Ermittlung der Werte-Gefährdungspaare
- Bewertung nach
  - Eintrittswahrscheinlichkeit
  - Auswirkungen
- Berechnung eines Risikowertes
- Klassifizierungsmethoden: quantitativ (schwer) oder qualitativ (einfacher)

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse

Risiko-bewertung

- Ermittlung der Werte-Gefährdungspaare
- Bewertung nach
  - Eintrittswahrscheinlichkeit
  - Auswirkungen
- Berechnung eines Risikowertes
- Klassifizierungsmethoden: quantitativ (schwer) oder qualitativ (einfacher)

Wahrscheinlichkeit	Beschreibung
Hoch	einmal pro Monat oder öfter
Mittel	Einmal pro Jahr
Gering	Alle paar Jahre (z.B. 3-5)

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse

Risiko-bewertung

- Ermittlung der Werte-Gefährdungspaare
- Bewertung nach
  - Eintrittswahrscheinlichkeit
  - Auswirkungen
- Berechnung eines Risikowertes
- Klassifizierungsmethoden: quantitativ (schwer) oder qualitativ (einfacher)

Wahrscheinlichkeit	Beschreibung
Hoch	einmal pro Monat oder öfter
Mittel	Einmal pro Jahr
Gering	Alle paar Jahre (z.B. 3-5)

Schaden	Beschreibung
Hoch	100.001 oder mehr
Mittel	10.001 bis 100.000 EUR
Gering	Bis 10.000 EUR

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse

Risiko-bewertung

- Ermittlung der Werte-Gefährdungspaare
- Bewertung nach
  - Eintrittswahrscheinlichkeit
  - Auswirkungen
- Berechnung eines Risikowertes
- Klassifizierungsmethoden: quantitativ (schwer) oder qualitativ (einfacher)

Wahrscheinlichkeit	Beschreibung
Hoch	einmal pro Monat oder öfter
Mittel	Einmal pro Jahr
Gering	Alle paar Jahre (z.B. 3-5)

Schaden	Beschreibung
Hoch	100.001 oder mehr
Mittel	10.001 bis 100.000 EUR
Gering	Bis 10.000 EUR

Risiko	Beschreibung
Hoch	Sofort Maßnahmen finden!
Mittel	Mittelfristig vermindern
Gering	Akzeptieren oder vermindern

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse

Wahrscheinlichkeit	Beschreibung
Hoch	einmal pro Monat oder öfter
Mittel	Einmal pro Jahr
Gering	Alle paar Jahre (z.B. 3-5)

Schaden	Beschreibung
Hoch	100.001 oder mehr
Mittel	10.001 bis 100.000 EUR
Gering	Bis 10.000 EUR

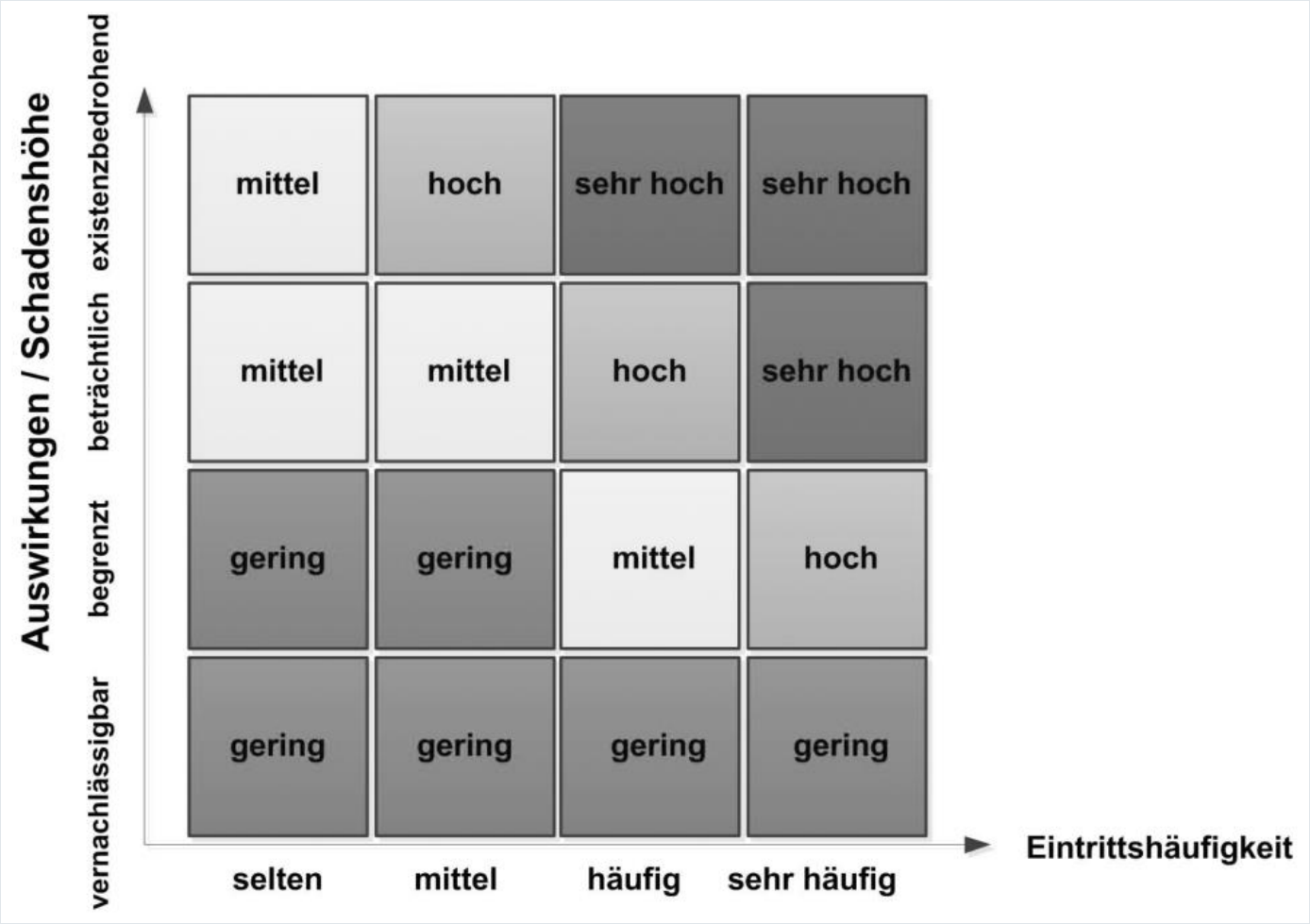
Risiko	Beschreibung
Hoch	Sofort Maßnahmen finden!
Mittel	Mittelfristig vermindern
Gering	Akzeptieren oder vermindern

Risikomatrix

Schaden				
	Hoch	Mittel	Hoch	Hoch
	Mittel	Gering	Mittel	Hoch
	Gering	Gering	Gering	Mittel
		Gering	Mittel	Hoch
		Wahrscheinlichkeit		

RISIKOBEWERTUNG

Wesentliche Schritte einer Risikoanalyse



Quelle: BSI Standard 200-3

RISIKOBEHANDLUNG

Wesentliche Schritte einer Risikoanalyse

Risiko-behandlung

- Gruppieren nach Schwere des Risikos
- Festlegen von Behandlungsoptionen
  - Risikoakzeptanz
  - Risikotransfer
  - Risikovermeidung
  - Risikoreduktion

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/Zertifizierte-Informationssicherheit/IT-Grundschutzschulung/Online-Kurs-Notfallmanagement/4_RisikenAnalysieren/4_StrategienWaehlen/StrategienWaehlen_node.html

MAßNAHMEN

Wesentliche Schritte einer Risikoanalyse

Maßnahmen

- Definition von konkreten Maßnahmen
  - Risikoakzeptanz -> Nichts tun
  - Risikotransfer -> Versicherung / Auslagerung an Dienstleister
  - Risikovermeidung -> Entfernen
  - Risikoreduktion -> Maßnahmen definieren
- Maßnahmennachverfolgung
- Verantwortlichkeiten definieren

BEISPIEL EINER RISKOANALYSE

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

Risiko	Wert	EW	Schaden	Risiko
Nicht-Verfügbarkeit des Standorts durch Brand	Standort			
Internetausfall am Standort	Standort			
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall			
Unbefugter Zugang zu Information am Laptop	Endgerät			
Erfolgreiche Malware-Infektion	Netzlaufwerk			
Erfolgreiche Malware-Infektion	Endgerät			
Unbefugter Zugriff auf Backup-Disks	Backup			
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup			
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup			
Langfristiger Ausfall von Schlüsselpersonal	Personal			

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

Risiko	Wert	EW	Schaden	Risiko
Nicht-Verfügbarkeit des Standorts durch Brand	Standort	Gering	Hoch	
Internetausfall am Standort	Standort	Mittel	Gering	
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall	Mittel	Mittel	
Unbefugter Zugang zu Information am Laptop	Endgerät	Gering	Mittel	
Erfolgreiche Malware-Infektion	Netzlaufwerk	Gering	Hoch	
Erfolgreiche Malware-Infektion	Endgerät	Gering	Gering	
Unbefugter Zugriff auf Backup-Disks	Backup	Gering	Hoch	
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup	Gering	Mittel	
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup	Gering	Hoch	
Langfristiger Ausfall von Schlüsselpersonal	Personal	Mittel	Hoch	

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

Schaden				
	Hoch	Mittel	Hoch	Hoch
	Mittel	Gering	Mittel	Hoch
	Gering	Gering	Gering	Mittel
		Gering	Mittel	Hoch
		Wahrscheinlichkeit		

Risiko	Wert	EW	Schaden	Risiko
Nicht-Verfügbarkeit des Standorts durch Brand	Standort	Gering	Hoch	Mittel
Internetausfall am Standort	Standort	Mittel	Gering	Gering
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall	Mittel	Mittel	Mittel
Unbefugter Zugang zu Information am Laptop	Endgerät	Gering	Mittel	Gering
Erfolgreiche Malware-Infektion	Netzlaufwerk	Gering	Hoch	Mittel
Erfolgreiche Malware-Infektion	Endgerät	Gering	Gering	Gering
Unbefugter Zugriff auf Backup-Disks	Backup	Gering	Hoch	Mittel
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup	Gering	Mittel	Gering
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup	Gering	Hoch	Mittel
Langfristiger Ausfall von Schlüsselpersonal	Personal	Mittel	Hoch	Hoch

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

Risiko	Wert	EW	Schaden	Risiko
Langfristiger Ausfall von Schlüsselpersonal	Personal	Mittel	Hoch	Hoch
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup	Gering	Hoch	Mittel
Unbefugter Zugriff auf Backup-Disks	Backup	Gering	Hoch	Mittel
Nicht-Verfügbarkeit des Standorts durch Brand	Standort	Gering	Hoch	Mittel
Erfolgreiche Malware-Infektion	Netzlaufwerk	Gering	Hoch	Mittel
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall	Mittel	Mittel	Mittel
Unbefugter Zugang zu Information am Laptop	Endgerät	Gering	Mittel	Gering
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup	Gering	Mittel	Gering
Internetausfall am Standort	Standort	Mittel	Gering	Gering
Erfolgreiche Malware-Infektion	Endgerät	Gering	Gering	Gering

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

Risiko	Wert	EW	Schaden	Risiko	Behandlung	Maßnahme
Langfristiger Ausfall von Schlüsselpersonal	Personal	Mittel	Hoch	Hoch	Reduktion / Transfer	
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup	Gering	Hoch	Mittel	Reduktion	
Unbefugter Zugriff auf Backup-Disks	Backup	Gering	Hoch	Mittel	Akzeptieren	
Nicht-Verfügbarkeit des Standorts durch Brand	Standort	Gering	Hoch	Mittel	Akzeptieren	
Erfolgreiche Malware-Infektion	Netzlaufwerk	Gering	Hoch	Mittel	Reduktion	
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall	Mittel	Mittel	Mittel	Vermeidung	
Unbefugter Zugang zu Information am Laptop	Endgerät	Gering	Mittel	Gering	Akzeptieren	
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup	Gering	Mittel	Gering	Reduktion	
Internetausfall am Standort	Standort	Mittel	Gering	Gering	Reduktion	
Erfolgreiche Malware-Infektion	Endgerät	Gering	Gering	Gering	Akzeptieren	

DURCHFÜHRUNG EINER RISIKOANALYSE

Beispiel einer Risikoanalyse

+verantwortliche Person
+Zeithorizont

Risiko	Wert	EW	Schaden	Risiko	Behandlung	Maßnahme
Langfristiger Ausfall von Schlüsselpersonal	Personal	Mittel	Hoch	Hoch	Reduktion / Transfer	Aufbau neues Personal / Dienstleister
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Computerprogramme	Backup	Gering	Hoch	Mittel	Reduktion	Backups Read-Only setzen
Unbefugter Zugriff auf Backup-Disks	Backup	Gering	Hoch	Mittel	Akzeptieren	-
Nicht-Verfügbarkeit des Standorts durch Brand	Standort	Gering	Hoch	Mittel	Akzeptieren	-
Erfolgreiche Malware-Infektion	Netzlaufwerk	Gering	Hoch	Mittel	Reduktion	Spezialsoftware anschaffen
Sicherheitslücken in der Firewall und Zugriff auf internes Netz	Firewall	Mittel	Mittel	Mittel	Vermeidung	Austausch Firewall
Unbefugter Zugang zu Information am Laptop	Endgerät	Gering	Mittel	Gering	Akzeptieren	-
Absichtliche oder unabsichtliche Veränderung von Backup-Daten durch Personen	Backup	Gering	Mittel	Gering	Reduktion	Backups Read-Only setzen
Internetausfall am Standort	Standort	Mittel	Gering	Gering	Reduktion	Anschaffung 2. Leitung
Erfolgreiche Malware-Infektion	Endgerät	Gering	Gering	Gering	Akzeptieren	-

WE SEARCH FOR GREATNESS.

BDO