Danke für die Einladung!

Was tun für mehr IT-Sicherheit?

Vorstellung des Referenten Sönke Wehrend

- IT-Security- Beauftragter, -Manager und -Auditor (TÜV)
- IT-Compliance Manager (PRW)
- ISO 27005 Risk Manager (PECB)
- Fachkraft für Datenschutz (DEKRA)

- Geschäftsführender Gesellschafter W&B GmbH und W&B Plus GmbH

Vorstellung W&B Plus GmbH
Datenschutz

- Informationssicherheits- und Datenschutzberatung
- zertifizierte Fachkräfte und Jurist*innen
- Stellung des externen Datenschutz-Beauftragten
- unabhängige IT-Sicherheits-IST-Analyse (ITQ)
- Mitarbeiter-Awareness: E-Learning Kampagnen zu Informationssicherheit und Datenschutz
- Gründung: 2018

Vorstellung W&B GmbH: IT-Systemhaus

- Managed-IT-Service:
  Automatisierung und Überwachung von IT-Sicherheitsmaßnahmen,
  Verfügbarkeit von IT-Fachkräften,
  laufende Betreuung und Dokumentation
- IT-Projekte:
  IT-Infrastuktur, Cloud-Migration,
  M365, Cloud-Telefonie
  Planung, Beschaffung und Betreuung
- Gründung: 1995
- 70 engagierte Kolleg*innen

IHRE FRAGEN

- Wie kann ich mich auf Cyberangriffe vorbereiten?
- Welche IT-Schutzmaßnahmen sind aktuell ein „Must-have“, welche ein „No-Go“?
- Wie erstelle ich eine Risikoanalyse bzw. wer hilft mir dabei?
- Wie kann ich auf Kundenanforderungen eingehen? (Zertifizierungen, Datenschutz)
- Was mache ich, wenn ich betroffen bin und wen muss ich informieren?
- Wer hilft mir, wenn ich betroffen bin?
- Wie erfolgt die Kommunikation im Fall eines Angriffs?
- Wie bereite ich mich auf den Notfall vor? (Notfallpläne, Aufrechterhalten der Kernprozesse, Neuaufbau, Wiederanfahren)

IHRE FRAGEN

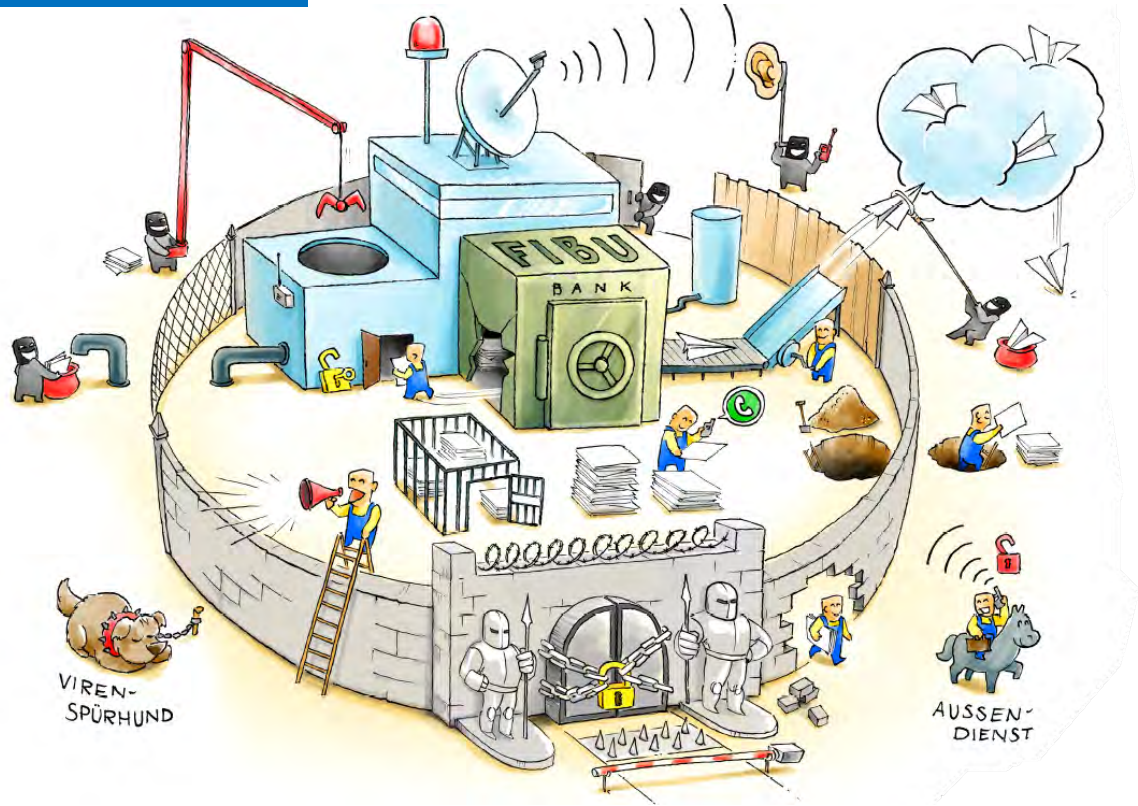
- **Was mache ich, wenn ich betroffen bin?**
  Wen muss ich informieren?
  - Wer hilft mir, wenn ich betroffen bin?
  - Wie erfolgt die Kommunikation im Fall eines Angriffs?
- **Wie kann ich mich auf Cyberangriffe vorbereiten?**
  - Wie bereite ich mich auf den Notfall vor?
    (Notfallpläne, Aufrechterhalten der Kernprozesse, Neuaufbau, Wiederanfahren)
  - Wie erstelle ich eine Risikoanalyse bzw. wer hilft mir dabei?
- **Wie kann ich auf Kundenanforderungen eingehen?**
  (Zertifizierungen, Datenschutz)
- **Welche IT-Schutzmaßnahmen sind aktuell ein „Must-have“, welche ein „No-Go“?**

Was mache ich, wenn ich betroffen bin?

Keine Vorbereitung?
Keine Hilfe!
Keine Wiederherstellung!
Keine Chance!

Bild: Freepik.com / cookie_studio

Unternehmensrisiken Datensicherheit



© ITQ Institut für Technologiequalität

Eine ITQ Graphik

Wie kann ich mich auf Cyberangriffe vorbereiten?

strukturierte Vorbereitung:
analysieren, planen,
dokumentieren …

Wie kann ich mich auf Cyberangriffe vorbereiten?

Handout!

BSI Arbeitspapier

Maßnahmenkatalog Ransomware

Risikoanalyse: Inventarbasiert oder **prozessbasiert**?

Risiko-Einstufung

Risikoklassen		Wert
1		
2		
3		
4		
5		
Eintrittswarscheinlichkeit		**Wert**
1		
2		
3		

Farbskala			

Risiko-Einstufung

Beispielannahmen und -ergebnisse aus einem Messeworkshop (IT FOR BUSINESS)

Risikoklassen			Wert
1	bestandsgefährdendes Risiko	≥	150.000,00 €
2	schwerwiegendes Risiko	≥	50.000,00 €
3	mittleres Risiko	≥	2.500,00 €
4	geringes Risiko	≥	500,00 €
5	Bagatellrisiko	≥	- €
Eintrittswarscheinlichkeit			**Wert**
1	gering	≤	5%
2	mittel	≤	20%
3	hoch	>	20%

Farbskala			
bestandsgefährdendes Risiko	11	12	13
schwerwiegendes Risiko	21	22	23
mittleres Risiko	31	32	33
geringes Risiko	41	42	43
Bagatellrisiko	51	52	53
	gering	mittel	hoch

Risiko-Analyse

ID	Risikobezeichnung (Ereignis)	Mögliche Risikoursachen	EW %	Tragweite/Schadenshöhe (€)	Risikowert
R1				€	
R2				€	
R3				€	
R12				€	
R13				€	
R31				€	
R32				€	
R33				€	

Risiko-Analyse

Beispielannahmen und -ergebnisse aus einem Messeworkshop (IT FOR BUSINESS)

ID	Risikobezeichnung (Ereignis)	Mögliche Risikoursachen	EW %	Tragweite/Schadenshöhe (€)	Risikowert
R1	Feuer		0,1	4.500.000,00 €	inakzeptabel
R2	Elementarschäden		0,5	1.000.000,00 €	inakzeptabel
R3	Einbruch/Diebstahl		2	500.000,00 €	inakzeptabel
R12	Personalausfall Verwaltung		10	36.000,00 €	prüfen
R13	Personalausfall Assistenz		10	25.000,00 €	prüfen
	Ausfall IT				
R31	Stromausfall	Versorgerprobleme	7	25.800,00 €	prüfen
R32	Datenverlust	Krypto-Trojaner	20	75.000,00 €	inakzeptabel
R33	Datenschutzvorfall	Krypto-Trojaner	20	200.000,00 €	inakzeptabel

Risiko-Behandlung

ID	Risikobezeichnung (Ereignis)	EW %	Schadens-höhe (€)	Ergebnis	empfohlene Maßnahme	Kosten der Maßnahme	EW %	Schadens-höhe (€)	Ergebnis
R1			€			€		€	
R2			€			€		€	
R3			€			€		€	
R4			€			€		€	
R12			€			€		€	
R13			€			€		€	
R14			€			€		€	
R15			€			€		€	
R16			€			€		€	
R31			€			€		€	
R32			€			€		€	
R33			€			€		€	
R34				- €					

Risiko-Behandlung

Beispielannahmen und -ergebnisse aus einem Messeworkshop (IT FOR BUSINESS)

ID	Risikobezeichnung (Ereignis)	EW %	Schadens-höhe (€)	Ergebnis	empfohlene Maßnahme	Kosten der Maßnahme	EW %	Schadens-höhe (€)	Ergebnis	Kommentar
R1	Berufsunfähigkeit	0,1	4.200.000 €	inakzeptabel	BU-Versicherung		0,1	1.000.000 €	inakzeptabel	Restschaden wird akzeptiert, da eine höhere Versicher-ung zu teuer ist.
R2	Feuer	0,1	1.000.000 €	inakzeptabel	Feuer-Versicherung	3.000 €	0,1	5.000 €	akzeptabel	
R3	Elementarschäden	0,5	500.000 €	inakzeptabel	Elementarschäden-Versicherung	500 €	0,5	5.000 €	akzeptabel	
R4	Einbruch/Diebstahl	2	500.000 €	inakzeptabel	Inventar-Versicherung, Einbruchsicherung, Alarmanlage	2.000 €	2	5.000 €	akzeptabel	
R12	Personalausfall Verwaltung	10	36.000 €	prüfen			10	36.000 €	prüfen	
R13	Personalausfall Assistenz	10	25.000 €	prüfen			10	25.000 €	prüfen	
R14	Ausfall einzelner EDV-Systeme	5	3.000 €	akzeptabel			5	3.000 €	akzeptabel	
R15	Totalschaden Produktionsanlage	0,1	70.000 €	akzeptabel			0,1	70.000 €	akzeptabel	
R16	Ausfall Produktionsanlage	2	10.000 €	akzeptabel			2	10.000 €	akzeptabel	
R31	Ausfall IT	7	30.000 €	prüfen	durch R32 und R33 erledigt	- €	1	10.000 €	akzeptabel	
R32	Datenverlust	4	150.000 €	inakzeptabel	Datensicherungskonzept erstellen und umsetzen, Managed Backup mit verschlüsselter Replikation in sicheres Rechenzentrum inkl. laufender Überwachung	1.800 €	0,1	3.000€	akzeptabel	
R33	Datenschutzvorfall	2	200.000 €	inakzeptabel	IT-Sicherheits-Audit: Firewall, AV auf EDR Umstellung, Patch-Management für Server und Clients, Dokumentation, alles inkl. laufender Überwachung	3.000 €	0,1	5.000 €	akzeptabel	
R34				- €						

Wie kann ich mich auf Cyberangriffe vorbereiten?

regelmäßig prüfen,
Schwachstellen finden,
Maßnahmen anpassen

ITQ-Basisprüfung

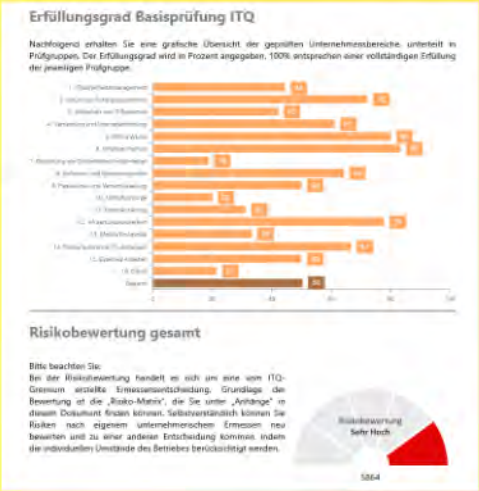
ITQ-Basisprüfung

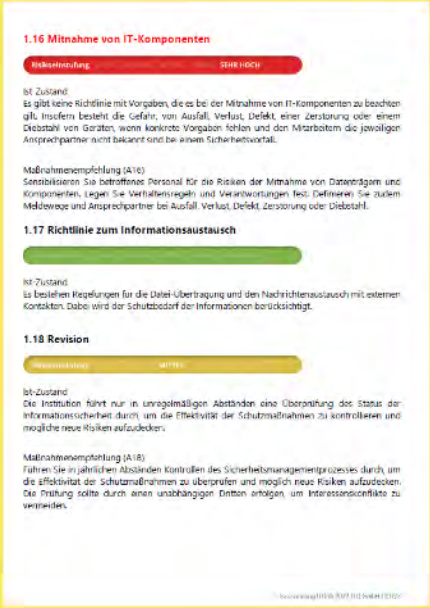
Leistung

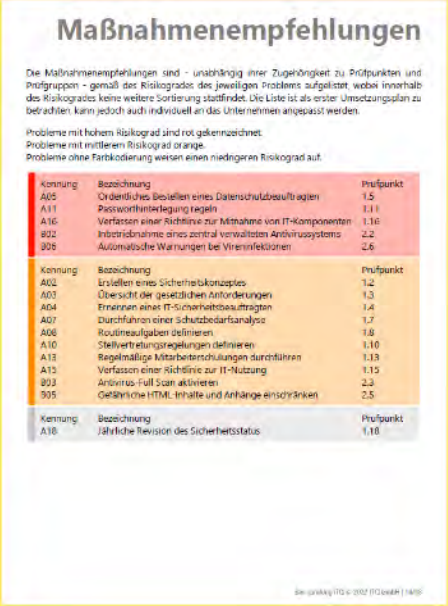
- Bundesweiter, anerkannter Standard für IT/-Informationssicherheit
- Klein- und mittelstandsgerechte Prüfung der Informationssicherheit
- Detaillierter Ergebnis- und Managementbericht
- Kosteneffiziente Vorgehensweise, idealer Einstieg. Vorteile bei späterer Zertifizierung
- Konkrete Handlungsempfehlungen
- Grundlage jeder Zertifizierung

© ITQ Institut für Technologiequalität

Unabhängige Basisprüfung: ITQ-Prüfbericht







© ITQ Institut für Technologiequalität

Unabhängige Prüfung des IST-Zustandes der IT

ITQ steht für : Höchste IT-Qualität im deutschsprachigen Mittelstand

ITQ
Institut für Technologiequalität

Audit / Gütesiegel

1. Ist-Analyse

Der erste Schritt in Richtung hoher und nachweisbarer IT-Sicherheit.

2. Optimierung

Setzen Sie zusammen mit Ihrem ITQ-Kompetenzpartner Handlungsempfehlungen um.

3. Kontrolle

Lassen Sie sich den Erfolg Ihrer Maßnahmen messbar nachweislich bestätigen.

4. Zertifizierung

Mit den Zertifikaten des ITQ belegen Sie geprüft sichere IT in Ihrem Unternehmen.

5. Zukunftssicher

ITQ-Zertifikate schaffen die Basis für internationale Standards wie ISO und DIN.

IT-Schutzmaßnahmen: „No-Gos“ und „Must-haves“

- Kein Backup – kein Mitleid!
- Kein Wartungsvertrag – kein Support!
- Kein Überblick – keine Sicherheit!

- Verantwortung für die IT-Sicherheit zurück an die Geschäftsführung
- Entscheidungsvorlagen in - für die Geschäftsführung - geeigneter Form beschaffen

Was tun für mehr IT-Sicherheit?

Danke für Ihre Aufmerksamkeit.
Rückfragen jederzeit gerne.

Bei Interesse sprechen Sie uns gerne an!

W&B Plus GmbH – Datenschutz

- Informationssicherheits- und Datenschutzberatung; Mitarbeiter-Awareness
- Stellung des externen Datenschutz-Beauftragten
- unabhängige IT-Sicherheits-IST-Analyse (ITQ)

Adresse: Steinmetzstraße 7, 23556 Lübeck
Telefon: 0451-202715-0
E-Mail: info@wb-datenschutz.de
Homepage: www.wb-datenschutz.de

W&B GmbH – IT-Systemhaus

- Managed-IT-Service
- IT-Security
- IT-Projekte: IT-Infrastuktur, Cloud-Migration, M365, Cloud-Telefonie, IT-Planung, -Beschaffung und -Betreuung

Adresse: Steinmetzstraße 7, 23556 Lübeck
Telefon: 0451 39988-0
E-Mail: info@wb-net.de
Homepage: www.wb-systemhaus.de