Informationssicherheits-Check
für Kommunen in NRW

Frank Wrede | Geschäftsführer | Bechtle Dortmund
03. Juni 2024

INFORMATIONSSICHERHEITS-CHECK
Ziele

- Transparente Darstellung des IT-Sicherheitsstatus
- Aufdecken von IT-Sicherheitslücken
- Erkennen von dringenden Handlungsbedarfen
- Erkennen regionaler Muster / Aufdecken von systemischen Fehlern
- Erstellen von praktischen und umsetzbaren Handlungsempfehlungen
- Erhöhung des IT-Sicherheitsstatus

INFORMATIONSSICHERHEITS-CHECK
Landesseitiges Unterstützungsangebot

Standardisiertes Vorgehen

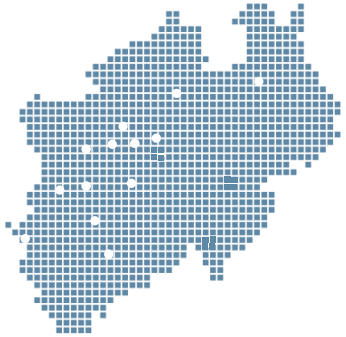
414 Kommunen

383 NRW-Städte und -Gemeinden
< 250.000 Einwohnerinnen und Einwohner
und 31 Kreise

kreisbezogene Vorgehensweise

Hohe Komplexität

bedarf individueller Betrachtung



13 NRW-Städte mit > 250.000 Einwohnerinnen und Einwohner
(Aachen, Bielefeld, Bochum, Bonn, Dortmund, Düsseldorf, Duisburg, Essen, Gelsenkirchen, Köln, Mönchengladbach, Münster, Wuppertal)

INFORMATIONSSICHERHEITS-CHECK | Vorgehen

- Interview nach BSI und ISACA Leitfaden
- Insgesamt 62 Prüffragen
  - angereichert um Bechtle Best-Practices
- Technische Stichproben der Systeme
  - AD (Pingcastle), LAN, E-Mail, Webserver, etc.
  - Schwachstellenanalyse der IT-Infrastruktur (Nessus)
- Sichtung der erforderlichen Richtlinien und Dokumentationen
- Maßnahmen und Empfehlungen zur Erhöhung des Schutzniveaus
- Adaptierbar in ein Informationssicherheitsmanagementsystem (ISMS)

Bundesamt für Sicherheit in der Informationstechnik

ISACA

INFORMATIONSSICHERHEITS-CHECK | Phasen

Bechtle Cyber Security Spezialist

PHASE 1

Vorgespräch inkl. OSINT

Zeitinvestition der Kommune
1 Stunde, remote

PHASE 2

Assessment

Zeitinvestition der Kommune: 2 Tage, vor Ort

PHASE 3

Nachbereitung, Auswertung, Analyse

PHASE 4

Ergebnis-präsentation

Zeitinvestition der Kommune
2 - 6 Stunden, vor Ort

INFORMATIONSSICHERHEITS-CHECK | Ergebnisbericht

Mehr als 100 Seiten Ergebnisbericht

- Darstellung der IST-Situation
- Konkrete Handlungsempfehlungen
- Beurteilung der Schwachstellen im Ampelsystem
  - keine Mängel (grün)
    - Zum Zeitpunkt der Beurteilung konnte kein Sicherheitsmangel festgestellt werden
  - Mängel (gelb)
    - Es liegt eine Sicherheitslücke vor, die mittelfristig behoben werden sollte. Die Vertraulichkeit, Integrität oder Verfügbarkeit der Informationen kann dadurch beeinträchtigt sein.
  - Schwerwiegende Mängel (rot)
    - Es wurde eine Sicherheitslücke identifiziert, die umgehend geschlossen werden sollte, da die Vertraulichkeit, die Integrität und / oder die Verfügbarkeit der Informationen stark gefährdet sind und erheblicher Schaden zu erwarten ist.
  - Nicht zu beurteilen (weiß)

INFORMATIONSSICHERHEITS-CHECK | Ergebnisbericht

	THEMENKOMPLEX	ERFÜLLUNGSGRAD MASSNAHMEN
A	Absicherung von Netzübergängen	A.1 A.2 A.3 A.4 A.5 A.6 A.7
B	Abwehr von Schadprogrammen	B.1 B.2 B.3
C	Inventarisierung der Systeme	C.1 C.2 C.3
D	Vermeidung von offenen Sicherheitslücken	D.1 D.2 D.3 D.4 D.5 D.6
E	Sichere Interaktion mit dem Internet	E.1 E.2 E.3 E.4 E.5 E.6
F	Logdatenerfassung und –Auswertung	F.1 F.2 F.3
G	Sicherstellung eines aktuellen Informationsstands	G.1 G.2
H	Bewältigung von Sicherheitsvorfällen	H.1 H.2 H.3 H.4
I	Sichere Authentisierung	I.1 I.2 I.3 I.4
J	Gewährleistung der Verfügbarkeit notwendiger Ressourcen	J.1 J.2 J.3
K	Durchführung Nutzerorientierter Maßnahmen	K.1 K.2 K.3
L	Sichere Nutzung sozialer Netzwerke	L.1 L.2 L.3
M	Durchführung von Penetrationstests	M.1 M.2 M.3
N	Sicherer Umgang mit Cloud-Anwendungen	N.1 N.2 N.3 N.4 N.5
B1	Erforderliche Basis-Sicherheitsrichtlinien	B-1.1

	THEMENKOMPLEX	ERFÜLLUNGSGRAD MASSNAHMEN
A	Absicherung von Netzübergängen	A.1 A.2 A.3 A.4 A.5 A.6 A.7
B	Abwehr von Schadprogrammen	B.1 B.2 B.3
C	Inventarisierung der Systeme	C.1 C.2 C.3
D	Vermeidung von offenen Sicherheitslücken	D.1 D.2 D.3 D.4 D.5 D.6
E	Sichere Interaktion mit dem Internet	E.1 E.2 E.3 E.4 E.5 E.6
F	Logdatenerfassung und –Auswertung	F.1 F.2 F.3
G	Sicherstellung eines aktuellen Informationsstands	G.1 G.2
H	Bewältigung von Sicherheitsvorfällen	H.1 H.2 H.3 H.4
I	Sichere Authentisierung	I.1 I.2 I.3 I.4
J	Gewährleistung der Verfügbarkeit notwendiger Ressourcen	J.1 J.2 J.3
K	Durchführung Nutzerorientierter Maßnahmen	K.1 K.2 K.3
L	Sichere Nutzung sozialer Netzwerke	L.1 L.2 L.3
M	Durchführung von Penetrationstests	M.1 M.2 M.3
N	Sicherer Umgang mit Cloud-Anwendungen	N.1 N.2 N.3 N.4 N.5
B1	Erforderliche Basis-Sicherheitsrichtlinien	B-1.1

Keine Mängel | Mängel | Schwerwiegende Mängel | Nicht zu beurteilen

INFORMATIONSSICHERHEITS-CHECK | Orientierung am BSI-Grundschutz

BSI-Grundschutz Kompendium

- Der Informationssicherheits-Check orientiert sich am BSI-Grundschutz-Kompendium
- Im Ergebnisbericht werden die jeweiligen BSI-Referenzen inklusive resultierender Handlungsempfehlungen aufgeführt
- Leitfaden erstellt in Zusammenarbeit mit der **Allianz für Cybersicherheit** und dem **BSI** (Bundesamt für Sicherheit in der Informationstechnik)

D.1 - Ein effizienter Prozess zum Schwachstellen- und Patchmanagement ist etabliert.	
Ergebnis	Mängel Es existieren regelmäßige Patchdays des Kunden, ein Schwachstellenmanagement wird allerdings nicht betrieben.
BSI-Referenzen	APP.2.1.A5 Sichere Konfiguration und Konfigurationsänderungen von Verzeichnis-diensten APP.2.3.A1 Planung und Auswahl von Backends und Overlays für OpenLDAP ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen OPS.1.1.3.A1 Konzept für das Patch- und Änderungsmanagement OPS.1.1.3.A2 Festlegung der Zuständigkeiten OPS.1.1.3.A3 Konfiguration von Autoupdate-Mechanismen OPS.1.1.7.A1 Anforderungsspezifikation für das Systemmanagement OPS.1.1.7.A2 Planung des Systemmanagements OPS.1.1.7.A3 Zeitsynchronisation für das Systemmanagement OPS.1.1.7.A4 Absicherung der Systemmanagement-Kommunikation OPS.1.1.7.A5 Gegenseitige Authentisierung von Systemmanagement-Lösung und zu verwaltenden Systemen OPS.1.1.7.A6 Absicherung des Zugriffs auf die Systemmanagement-Lösung SYS.2.1.A3 Aktivieren von Autoupdate-Mechanismen SYS.2.3.A4 Einspielen von Updates und Patches auf unixartigen Systemen SYS.2.3.A5 Sichere Installation von Software-Paketen SYS.3.2.1.A5 Updates von Betriebssystem und Apps

INFORMATIONSSICHERHEITS-CHECK | Projektablauf

29.01.2024 **Beauftragung** der Informations-sicherheits-Checks	07.02.2024 **Kick-Off** mit allen Behörden durch das MHKBD	12.02.2024 **Projektstart** mit Freischaltung der Hotline	Februar **POC** mit fünf Kommunen
Bis heute **Interessens-bekundung** 340 Kommunen	Bis heute **Terminiert** 180 Kommunen	Bis Juli **Terminierung** aller Kommunen	Bis Dezember **Umsetzung** aller Informations-sicherheits-Checks

INFORMATIONSSICHERHEITS-CHECK

Wo stehen wir heute?

Kommunen vollständig geplant: **180**

PHASE 1	PHASE 2 & PHASE 3		PHASE 4
Vorgespräch inkl. OSINT	Assessment	Nachbereitung, Auswertung, Analyse	Ergebnispräsentation

Geplant	Durchgeführt	Geplant	Durchgeführt	Geplant	Durchgeführt
85	95	152	28	173	7

Stand: 03. Juni 2024

UMSETZUNG | Erste Erkenntnisse

- Feststellung erheblicher technischer und organisatorischer Sicherheitsmängel
  - Netzwerke sind nicht segmentiert
  - Keine Multifaktorauthentifizierung
  - Kein Passwortmanagement, keine Passwortrichtlinien
  - Kein strukturiertes oder automatisiertes Schwachstellenmanagement
  - Kein Notfallhandbuch
  - Fehlende Dokumentation der Infrastrukturen
- IT-Sicherheitsrichtlinien sind nicht definiert oder nicht auf dem aktuellen Stand
- In NRW gibt es teilweise eine starke Verflechtung der Kommunen mit dem jeweiligen kommunalen Rechenzentrum
  - Zum Teil vollständige Auslagerung der zentralen IT-Services
  - Dies entbindet die Kommune nicht von der Umsetzung organisatorischer Sicherheitsmaßnahmen

NÄCHSTE SCHRITTE | Erste Erkenntnisse

- Von den **62** geprüften Kriterien ist bei den bisherigen Checks bei **20** bis **40** Kriterien ein schwerwiegender Mangel festgestellt worden (rote Ampel)
  - Es ist nicht möglich, alle Mängel gleichzeitig zu beheben
  - Besonders gravierende Mängel werden gesondert dargestellt
  - Aufzeigen von Quick-Wins (geringer Aufwand -> großer Nutzen)
  - Vorschlag für Priorisierung
  - Empfehlung: Projektmanagement und Umsetzungsplan zur Behebung aller Sicherheitslücken (mehrmonatige Laufzeit)
  - Konkrete und praktisch umsetzbare Handlungsempfehlungen

Zeit für Ihre Fragen.

Weitere Infos:
bechtle.com