Deutsche Telekom Security GmbH

Cyber Security Assessment

Kundenpräsentation | April 2020

ERLEBEN, WAS VERBINDET.

Cyber Security Assessment
Einführung

- Ermittlung und Bewertung des aktuellen ganzheitlichen IT-Security Levels auf Basis
  - verschiedener industrieller Anforderungen, Frameworks
  - internationaler Normen und Standards (z.B. NIST, ISO27001, BSI 200-x)
  - Best Practice des Telekom Konzerns
- Organisatorischer und technischer Fokus
- Erkennung von Schwachstellen (Gaps)
- Benennung geeigneter Handlungsempfehlungen und Priorisierungsvorschlag
- *Auf Wunsch: Einleitung von Lösungsansätzen auf Basis geeigneter Services/Produkte nach Abschluss des Workshops*

Cyber Security Assessment

Methodik

Assessment

In einem eintägigen Workshop fragen wir verschiedenen Anforderungen in unterschiedlichen Domänen ab, um so den aktuellen Ist-Zustand Ihres IT-Sicherheitslevels zu ermitteln.

Preparation

In Vorbereitung auf das Assessment bestimmen wir in einem Erstgespräch einen Termin, die Örtlichkeit, Teilnehmer sowie den restlichen Scope des Workshops.

Presentation

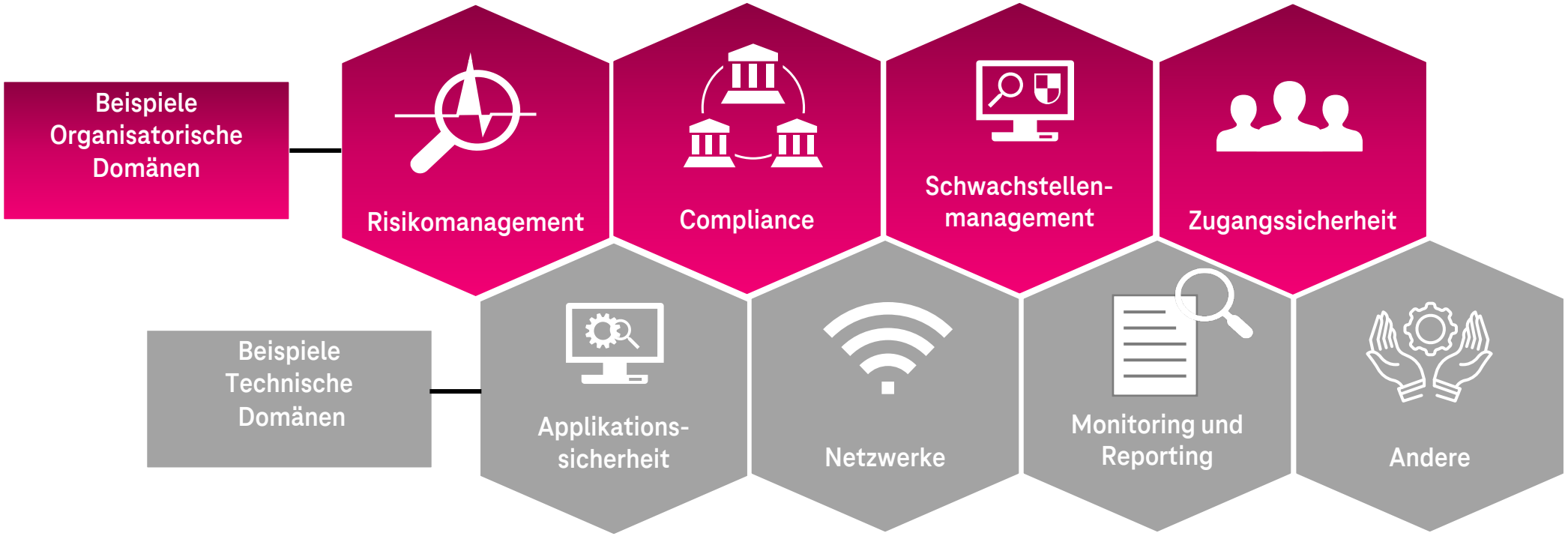
Im Anschluss an den Workshop erstellen wir eine Gap-Analyse und bewerten das Assessment. Zu identifizierten Gaps dokumentieren wir geeignete Handlungsempfehlungen präsentieren diese in einer separaten Session mit Ihnen.

Match making

Wir kombinieren die Assessment-Ergebnisse mit Ihren Anforderungen und stellen im Nachgang durch den verantwortlichen Vertriebler mögliche Lösungsansätze vor, die das IT-Sicherheitslevel Ihrer Organisation steigern können.

Cyber Security Assessment
Themenschwerpunkte

- Abfrage von ca. 170 Anforderungen aus 28 verschiedenen Domänen
- Berücksichtigung des kompletten DT Security Consulting Portfolio

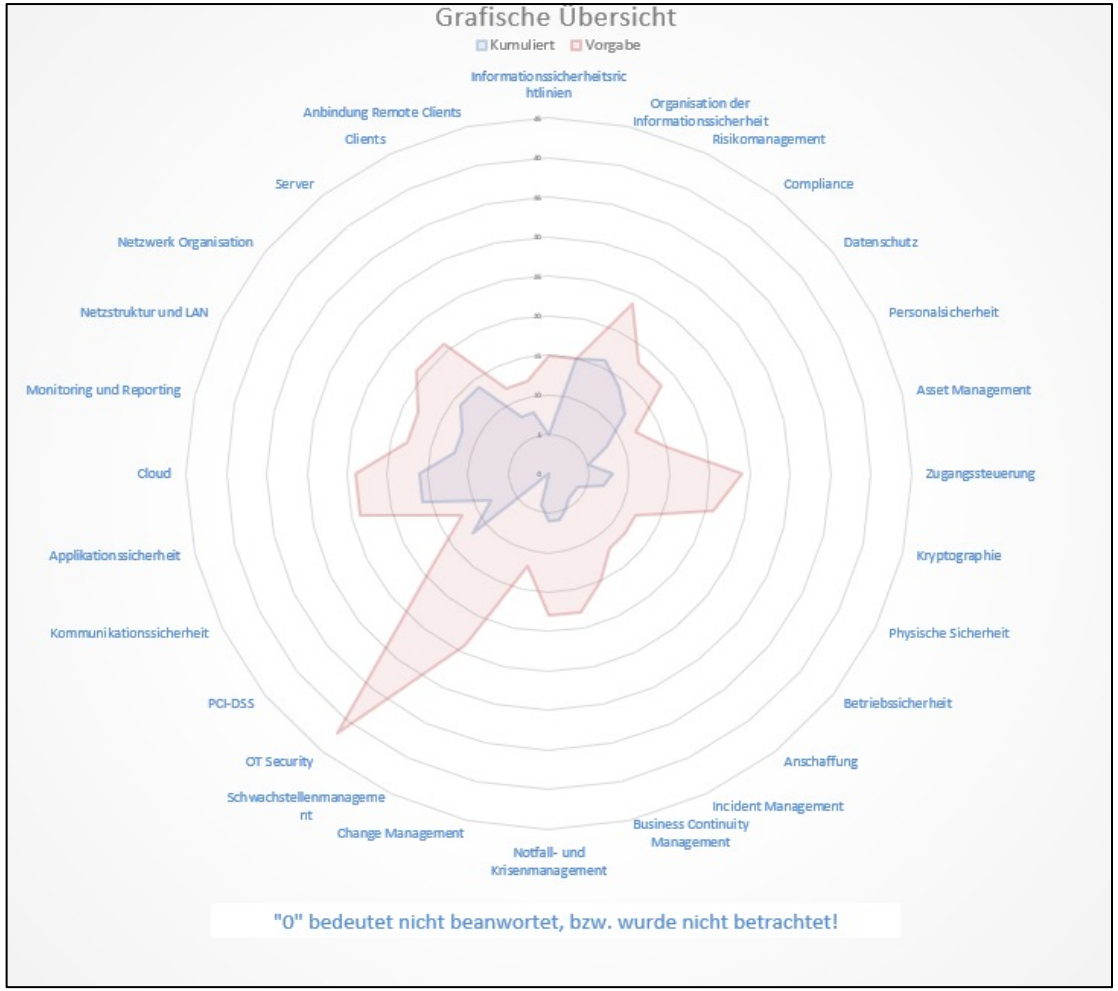


Auszug aus Domänenverzeichnis

Auszüge aus Cyber Security Assessment

004	ISO 27001	5.1.2	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Die Informationssicherheitsrichtlinie wird in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.		1	nicht erfüllt
005	NL	NL.002	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Mitarbeiter müssen über alle Änderungen an Informationssicherheitsrichtlinien proaktiv informiert werden.		1	nicht erfüllt
006	BSIG	OIS-1	STRATEGIE & GRC	Organisation der Informationssicherheit	Die Unternehmensleitung initiiert, steuert und überwacht ein Managementsystem zur Informationssicherheit (ISMS)		3	erfüllt
007	ISO 27001	6.1.1	STRATEGIE & GRC	Organisation der Informationssicherheit	Alle Informationssicherheitsverantwortlichkeiten sind festgelegt und zugewiesen, dokumentiert und an alle betroffenen Parteien kommuniziert		3	erfüllt
008	ISO 27001	6.1.2	STRATEGIE & GRC	Organisation der Informationssicherheit	Aufgaben und Verantwortlichkeiten sind so getrennt, dass Missbrauch oder Interessenskonflikte vermieden werden. (Separation of Duties)		3	erfüllt
009	ISO 27001	6.1.3	STRATEGIE & GRC	Organisation der Informationssicherheit	Es bestehen Regelungen, die den korrekten Umgang mit Strafverfolgungs und Aufsichtsbehörden regeln.		3	erfüllt
010	ISO 27001	6.1.4	STRATEGIE & GRC	Organisation der Informationssicherheit	Angemessene Kontakte mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen werden im		3	erfüllt
011	ISO27005	NL.003	STRATEGIE & GRC	Risikomanagement	Ein Risikomanagement im Unternehmes, welches alle Bereiche abdeckt, ist geregelt und etabliert.		2	teilweise erfüllt
012	BSIG	OIS-6	STRATEGIE & GRC	Risikomanagement	Eine Anweisung über das grundsätzliche Verfahren zur Identifikation, Analyse, Beurteilung und Behandlung von Risiken, insb IT-Risiken ist dokumentiert, kommuniziert und bereitgestellt.		2	teilweise erfüllt
013	ISO27005	NL.004	STRATEGIE & GRC	Risikomanagement	Eine Schutzbedarfsdefinition im Unternehmen (Beispiel: Standard, Mittel, Hoch, Kritisch) wurde vorgenommen.		2	teilweise erfüllt
014	ISO27005	NL.005	STRATEGIE & GRC	Risikomanagement	Alle Werte und Schutzziele des Unternehmens sind bezüglich ihrer Kritikalität bewertet und dokumentiert.		2	teilweise erfüllt

02	BSIG	OIS-2	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Die Informationssicherheitsrichtlinie enthält Sicherheitsziele und strategische Vorgaben, wie diese Ziele erreicht werden sollen.	0	1	nicht erfüllt	Organisatorisch
03	NL	NL.001	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Die Informationssicherheitsrichtlinie ist so formuliert, dass sie von allen Mitarbeitern verstanden und nachvollzogen werden können.	0	1	nicht erfüllt	Organisatorisch
04	ISO 27001	5.1.2	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Die Informationssicherheitsrichtlinie wird in geplanten Abständen oder jeweils nach erheblichen Änderungen überprüft werden, um sicherzustellen, dass sie nach wie vor geeignet, angemessen und wirksam sind.	0	1	nicht erfüllt	Organisatorisch
05	NL	NL.002	STRATEGIE & GRC	Informationssicherheitsrichtlinien	Mitarbeiter müssen über alle Änderungen an Informationssicherheitsrichtlinien proaktiv informiert werden.	0	1	nicht erfüllt	Organisatorisch
Handlungsempfehlung			Die Leitlinie zur Informationssicherheit ist ein wichtiges Grundsatzdokument der Leitung zu dem Stellenwert, den verbindlichen Prinzipien und dem anzustrebenden Niveau der Informationssicherheit in einer Institution.Für die betroffenen Mitarbeiter verständlich, wird auf wenigen Seiten beschrieben, welche Sicherheitsziele angestrebt und in welchem organisatorischen Rahmen diese umgesetzt werden sollen. - Was sollte in der Leitlinie zur Informationssicherheit festgelegt werden? - Der Geltungsbereich wird konkretisiert. - Die Bedeutung, die Informationssicherheit für eine Institution hat, wird hervorgehoben, etwa indem darauf hingewiesen wird, dass ein Ausfall der Informationstechnik oder Verletzungen der Vertraulichkeit und Integrität von Informationen die Existenz der Institution gefährden. - Die Verantwortung der Leitung wird betont, sowohl im Hinblick auf die Initiierung des Sicherheitsprozesses als auch auf dessen kontinuierliche Verbesserung. - Es wird auf einschlägige Gesetze und Regulierungsauflagen hingewiesen und die Mitarbeiter werden verpflichtet, diese zu beachten. - Es werden für die Informationssicherheit besonders wichtige Geschäftsprozesse genannt, etwa Produktionsabläufe, Forschungsverfahren oder Personalbearbeitung, und auf die strikte Einhaltung von Sicherheitsregeln hingewiesen. - Die Organisationsstruktur für Informationssicherheit und die Aufgaben der verschiedenen Sicherheitsverantwortlichen werden vorgestellt. - Sinnvoll ist auch der Hinweis auf Sicherheitsschulungen und Sensibilisierungsmaßnahmen.				


Grafische Übersicht
Kumuliert
Vorgabe
Informationssicherheitsrichtlinien
Organisation der Informationssicherheit
Risikomanagement
Compliance
Datenschutz
Personalsicherheit
Asset Management
Zugangssteuerung
Kryptographie
Physische Sicherheit
Betriebssicherheit
Anschaffung
Incident Management
Business Continuity Management
Notfall- und Krisenmanagement
Change Management
Schwachstellenmanagement
OT Security
PCI-DSS
Kommunikationssicherheit
Applikationssicherheit
Cloud
Monitoring und Reporting
Netzstruktur und LAN
Netzwerk Organisation
Server
Clients
Anbindung Remote Clients
"0" bedeutet nicht beanwortet, bzw. wurde nicht betrachtet!