Assignment #1: BSI Analyse

Lecture: D3.2: Information Security and Privacy
Abgabe: 20.10.2022 an: joerg.cosfeld@hs-duesseldorf.de

1. Der BSI Grundschutz gibt einen Unternehmen Leitlinien vor, um Ihre IT Sicherheit zu erhöhen. Versetzten Sie sich in die Lage der CIT der HSD und erstellen Sie eine Risikoanalyse eines Client PCs in Ihrem Unternehmen.

   Sie finden die entsprechenden Dokumente zur Erstellung der Analyse im Anhang dieses Dokumentes.

   (a) (5p.) Erstellen Sie eine Analyse für einen Standard Client PC.

   (b) (5p.) Erstellen Sie im gleichen Umfang eine Analyse zur Beurteilung eines Client PCs mit dem OS Windows 10.

   Tipp: In der Vorlesung wurde eine Analyse zur Nutzung eines Smartphones besprochen.

SYS.2.1 Allgemeiner Client

Nummer:		**Erfasst am:**		**Befragte Personen:**	
Bezeichnung:		**Erfasst durch:**		-"-	
Standort:				-"-	

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.1.A1	Sichere Benutzerauthentisierung	Basis								
SYS.2.1.A2	ENTFALLEN	Basis								
SYS.2.1.A3	Aktivieren von Autoupdate-Mechanismen	Basis								
SYS.2.1.A4	ENTFALLEN	Basis								
SYS.2.1.A5	ENTFALLEN	Basis								
SYS.2.1.A6	Einsatz von Schutzprogrammen gegen Schadsoftware	Basis								
SYS.2.1.A7	ENTFALLEN	Basis								
SYS.2.1.A8	Absicherung des Bootvorgangs	Basis								
SYS.2.1.A42	Nutzung von Cloud- und Online-Funktionen	Basis								
SYS.2.1.A9	Festlegung einer Sicherheitsrichtlinie für Clients	Standard								

SYS.2.1 Allgemeiner Client

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.1.A10	Planung des Einsatzes von Clients	Standard								
SYS.2.1.A11	Beschaffung von Clients	Standard								
SYS.2.1.A12	ENTFALLEN	Standard								
SYS.2.1.A13	Zugriff auf Ausführungsumgebungen mit unbeobachtbarer Codeausführung	Standard								
SYS.2.1.A14	Updates und Patches für Firmware, Betriebssystem und Anwendungen	Standard								
SYS.2.1.A15	Sichere Installation und Konfiguration von Clients	Standard								
SYS.2.1.A16	Deaktivierung und Deinstallation nicht benötigter Komponenten und Kennungen	Standard								
SYS.2.1.A17	ENTFALLEN	Standard								
SYS.2.1.A18	Nutzung von verschlüsselten Kommunikationsverbindungen	Standard								
SYS.2.1.A19	ENTFALLEN	Standard								

SYS.2.1 Allgemeiner Client

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.1.A20	Schutz der Administrationsverfahren bei Clients	Standard								
SYS.2.1.A21	Verhinderung der unautorisierten Nutzung von Rechnermikrofonen und Kameras	Standard								
SYS.2.1.A22	ENTFALLEN	Standard								
SYS.2.1.A23	Bevorzugung von Client-Server-Diensten	Standard								
SYS.2.1.A24	Umgang mit externen Medien und Wechseldatenträgern	Standard								
SYS.2.1.A25	ENTFALLEN	Standard								
SYS.2.1.A26	Schutz vor Ausnutzung von Schwachstellen in Anwendungen	Standard								
SYS.2.1.A27	Geregelte Außerbetriebnahme eines Clients	Standard								
SYS.2.1.A43	Lokale Sicherheitsrichtlinien für Clients	Standard								
SYS.2.1.A44	Verwaltung der Sicherheitsrichtlinien von Clients	Standard								

SYS.2.1 Allgemeiner Client

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.1.A28	Verschlüsselung der Clients	Hoch								
SYS.2.1.A29	Systemüberwachung und Monitoring der Clients	Hoch								
SYS.2.1.A30	Einrichten einer Referenzumgebung für Clients	Hoch								
SYS.2.1.A31	Einrichtung lokaler Paketfilter	Hoch								
SYS.2.1.A32	Einsatz zusätzlicher Maßnahmen zum Schutz vor Exploits	Hoch								
SYS.2.1.A33	Application Whitelisting	Hoch								
SYS.2.1.A34	Kapselung von sicherheitskritischen Anwendungen und Betriebssystemkomponenten	Hoch								
SYS.2.1.A35	Aktive Verwaltung der Wurzelzertifikate	Hoch								
SYS.2.1.A36	Selbstverwalteter Einsatz von SecureBoot und TPM	Hoch								
SYS.2.1.A37	Verwendung von Mehr-Faktor-Authentisierung	Hoch								
SYS.2.1.A38	Einbindung in die Notfallplanung	Hoch								

SYS.2.1 Allgemeiner Client

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.1.A39	Unterbrechungsfreie und stabile Stromversorgung	Hoch								
SYS.2.1.A40	Betriebsdokumentation	Hoch								
SYS.2.1.A41	Verwendung von Quotas für lokale Datenträger	Hoch								
SYS.2.1.A45	Erweiterte Protokollierung	Hoch								

SYS.2.2.3 Clients unter Windows 10

Nummer:		**Erfasst am:**		**Befragte Personen:**	
Bezeichnung:		**Erfasst durch:**		-"-	
Standort:				-"-	

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.2.3.A1	Planung des Einsatzes von Cloud-Diensten unter Windows 10	Basis								
SYS.2.2.3.A2	Auswahl und Beschaffung einer geeigneten Windows-10-Version	Basis								
SYS.2.2.3.A3	ENTFALLEN	Basis								
SYS.2.2.3.A4	Telemetrie und Datenschutzeinstellungen unter Windows 10	Basis								
SYS.2.2.3.A5	Schutz vor Schadsoftware unter Windows 10	Basis								
SYS.2.2.3.A6	Integration von Online-Konten in das Betriebssystem	Basis								
SYS.2.2.3.A7	ENTFALLEN	Standard								
SYS.2.2.3.A8	ENTFALLEN	Standard								

SYS.2.2.3 Clients unter Windows 10

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.2.3.A9	Sichere zentrale Authentisierung in Windows-Netzen	Standard								
SYS.2.2.3.A10	ENTFALLEN	Standard								
SYS.2.2.3.A11	Schutz der Anmeldeinformationen unter Windows 10	Standard								
SYS.2.2.3.A12	Datei- und Freigabeberechtigungen unter Windows 10	Standard								
SYS.2.2.3.A13	Einsatz der SmartScreen-Funktion	Standard								
SYS.2.2.3.A14	Einsatz des Sprachassistenten Cortana	Standard								
SYS.2.2.3.A15	Einsatz der Synchronisationsmechanismen unter Windows 10	Standard								
SYS.2.2.3.A16	Anbindung von Windows 10 an den Microsoft-Store	Standard								
SYS.2.2.3.A17	Keine Speicherung von Daten zur automatischen Anmeldung	Standard								
SYS.2.2.3.A18	Einsatz der Windows-Remoteunterstützung	Standard								

SYS.2.2.3 Clients unter Windows 10

Anforderung	Titel	Typ	ent-behrl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.2.2.3.A19	Sicherheit beim Fernzugriff über RDP	Standard								
SYS.2.2.3.A20	Einsatz der Benutzerkontensteuerung UAC für privilegierte Konten	Standard								
SYS.2.2.3.A21	Einsatz des Encrypting File Systems	Hoch								
SYS.2.2.3.A22	Verwendung der Windows PowerShell	Hoch								
SYS.2.2.3.A23	Erweiterter Schutz der Anmeldeinformationen unter Windows 10	Hoch								
SYS.2.2.3.A24	Aktivierung des Last-Access-Zeitstempels	Hoch								
SYS.2.2.3.A25	Umgang mit Fernzugriffsfunktionen der „Connected User Experience and Telemetry“	Hoch								