

Gefährdung Schweizer Spitäler gegenüber Cyberangriffen

MARTIN DARMS

Inhaltsverzeichnis

Danksagungen	5
Abstract	7
1 Einleitung	15
1.1 Motivation	15
1.2 Datenschutz	16
1.3 Forschungsfrage	16
1.3.1 Teilfragen	16
1.3.2 Gängige Behauptungen	16
2 Grundlagen	18
2.1 Schwachstellen	18
2.1.1 Definition von Schwachstellen	18
2.1.2 Historischer Hintergrund von Schwachstellen	18
2.1.3 Entwicklung der Schwachstellen	18
2.1.4 Vermeidung von Schwachstellen	20
2.1.5 Kosten von nicht behobenen Schwachstellen	21
2.2 Bedrohungslagen durch Cyberangriffe	22
2.3 Mögliche Angriffsvarianten	23
2.3.1 Verletzung der Vertraulichkeit	23
2.3.2 Verletzung der Integrität	24
2.3.3 Verletzung der Verfügbarkeit	24
2.3.4 Mögliche Angreifer	24
3 Methodisches Vorgehen	25
3.1 Vorgehen	25
3.1.1 Auswahl des Werkzeugs	25
3.1.2 Kennenlernen des Messwerkzeugs	26
3.1.3 Auswahl der Spitäler oder Institutionen im Gesundheitswesen	26
3.1.4 Rechtliche Abklärungen	27
3.1.5 Durchführung eines Pilotprojekts in Deutschland	27
3.1.6 Externes Scannen der Spitalnetze	27
3.1.7 Internes Scannen der Spitalnetze	28
3.1.8 Auswerten der Resultate	29
3.2 Gefährdungsindex – HVX	29
3.3 Literaturrecherche	30
4 Kriterien der Datenerhebung und Auswertung	35
4.1 Übersicht	35
4.1.1 Ziele von Penetration-Tests	35
4.1.2 Ziele von Vulnerability-Scannern	35

4.2	Elementare Gefährdungen	36
4.3	Datenerhebung durch Beobachtung während des Scannens	36
4.4	Auswertung nach Spitaltyp	36
4.5	Beteiligte Spitäler	37
5	Ergebnisse	39
5.1	Vorbemerkungen	39
5.2	Externe Scans	39
5.2.1	Resultate Spital K3	39
5.2.1.1	Vergleich potenzieller versus effektiv gefundene Schwachstellen ...	39
5.2.2	Resultate Spital K1	40
5.2.2.1	Vergleich potenzieller versus effektiv gefundene Schwachstellen ...	40
5.2.3	Resultate Schweizer Spitäler	41
5.2.4	Zusätzlicher externer Sicherheitstest – Logjam-Attacke	42
5.3	Interne Scans	45
5.4	Vergleich der Resultate mit einer Referenzmessung	46
5.4.1	Resultate des externen Scans	46
5.4.1.1	CH Durchschnitt – Deutschland Referenzklinik	46
5.4.1.2	Eins-zu-eins-Vergleich CH Spital – Referenzklinik D	47
5.4.2	Resultate der internen Scans	48
5.5	Zusammenfassung der Messungen und Statistik	49
5.5.1	Messungen in Schweizer Spitalern	49
5.5.2	Messungen in Schweizer Spitalern und in der Referenzklinik	49
5.6	Resultate im Überblick	49
5.7	Behauptungen und deren Beurteilungen	51
6	Schlussfolgerung und Ausblick	52
6.1	Verantwortlichkeiten und Kosten eines Cyberangriffes	53
7	Best Practices	55
7.1	Übersicht Massnahmen gegen Cyberangriffe	55
7.1.1	Best Practices – Liste für Spitäler	55
7.1.2	Best Practices – Liste für Medizingerätehersteller	56
7.2	IT-Standards und -Richtlinien – ISO 27000	57
7.2.1	IT-Grundschatz-Kataloge	57
7.2.2	ISO/IEC 27000:2016	57
7.2.3	ISO/IEC 27001:2013	57
7.2.4	ISO/IEC 27002:2013	58
7.2.5	ISO/IEC 27799:2008	58
7.2.6	ISO/IEC 27789:2013	58
7.2.7	ISO 22600-1:2015-02	59
7.2.8	ISO 22857:2013	59

7.2.9	IEC EN 80001-1:2010	59
7.3	Mitarbeiter schulen	60
7.4	Sicherheitskonzept mit verschiedenen Zonen	60
7.5	Benutzerrollen	63
7.6	Virtuelle Server	63
7.7	Aktives Patch-Management	63
7.8	Veraltete Betriebssysteme meiden	64
7.9	Zusatzgeräte wie USB-Ports sperren	64
7.10	Remotезugang von Drittfirmit einschränken	64
7.11	Backup, Backup, Backup	64
7.12	Schwachstellen-Management-Tools	64
7.13	Unabhängige Pen-Tests durchführen	65
7.14	Standard-SW verwenden	65
7.15	Diverse Tipps	65
	Literaturverzeichnis	66
	Abbildungsverzeichnis	70
	Abkürzungsverzeichnis	72
	Glossar	74
	Anhang	78
	Anhang A.1 – Messresultate – extern	78
	Extern K1	78
	Extern K2	79
	Extern K3	80
	Extern K4	81
	Extern K5	82
	Extern K6	83
	Extern K7	83
	Anhang A.2 – Messresultate – intern	84
	Intern K1	84
	Intern K2	85
	Intern K3	86
	Intern K4	87
	Intern K5	88
	Intern K6	89
	Intern K7	90
	Messresultate interner Scan – Beispiel	91

Inhaltsverzeichnis

Anhang A.3 – Referenzklinik Auswertung Medizintechnik	92
Anhang B – Verwendete Tools	92
Anhang C – Liste der Datenschutzverletzungen in den USA	93
Anhang D – Liste der Datenschutzverletzungen weltweit	102