

Nico Ohlig

IT-Security für KMU. Praxisnahe
Maßnahmen und Empfehlungen zur
grundlegenden Absicherung der IT-Systeme
in kleinen und mittelständischen
Unternehmen

Bachelorarbeit

BEI GRIN MACHT SICH IHR WISSEN BEZAHLT



- Wir veröffentlichen Ihre Hausarbeit, Bachelor- und Masterarbeit
- Ihr eigenes eBook und Buch - weltweit in allen wichtigen Shops
- Verdienen Sie an jedem Verkauf

Jetzt bei www.GRIN.com hochladen
und kostenlos publizieren



Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de/> abrufbar.

Dieses Werk sowie alle darin enthaltenen einzelnen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsschutz zugelassen ist, bedarf der vorherigen Zustimmung des Verlanges. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen, Auswertungen durch Datenbanken und für die Einspeicherung und Verarbeitung in elektronische Systeme. Alle Rechte, auch die des auszugsweisen Nachdrucks, der fotomechanischen Wiedergabe (einschließlich Mikrokopie) sowie der Auswertung durch Datenbanken oder ähnliche Einrichtungen, vorbehalten.

Impressum:

Copyright © 2021 GRIN Verlag
ISBN: 9783346460370

Dieses Buch bei GRIN:

<https://www.grin.com/document/1037239>

Nico Ohlig

IT-Security für KMU. Praxisnahe Maßnahmen und Empfehlungen zur grundlegenden Absicherung der IT-Systeme in kleinen und mittelständischen Unternehmen

GRIN - Your knowledge has value

Der GRIN Verlag publiziert seit 1998 wissenschaftliche Arbeiten von Studenten, Hochschullehrern und anderen Akademikern als eBook und gedrucktes Buch. Die Verlagswebsite www.grin.com ist die ideale Plattform zur Veröffentlichung von Hausarbeiten, Abschlussarbeiten, wissenschaftlichen Aufsätzen, Dissertationen und Fachbüchern.

Besuchen Sie uns im Internet:

<http://www.grin.com/>

<http://www.facebook.com/grincom>

http://www.twitter.com/grin_com

IT-Security für KMU

Praxisnahe Maßnahmen und Empfehlungen zur grundlegenden Absicherung der IT-Systeme in kleinen und mittelständigen Unternehmen am Beispiel eines Referenzunternehmens

Bachelorarbeit von

Nico Ohlig

Verfasser: Nico Ohlig

Abgabedatum: 12. April 2021

FACHHOCHSCHULE SÜDWESTFALEN

Fachbereich Elektrotechnik und Informationstechnologie

Hinweis:

Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestotrotz beziehen sich die Angaben auf Angehörige aller Geschlechter.

Kurzzusammenfassung

In der vorhergehenden Seminararbeit zum Thema „Motivation und Ablauf cyberkrimineller Angriffe in produzierenden Unternehmen“ wurden die wichtigsten Aspekte und Grundlagen zur Beschreibung der Problemstellung gegeben. Auf Basis der dargelegten Sachverhalte und den aus der Presse entnommenen Informationen zur Entwicklung der allgemeinen Bedrohungslage ist davon auszugehen, dass die Wahrscheinlichkeit zielgerichteter Angriffe auf ein jedes Unternehmen zunehmend steigt. Auch und vor allem Unternehmen aus dem Bereich KMU (kleine und mittelständige Unternehmen) sind aufgrund der steigenden Bedrohung durch cyberkriminelle Angriffe eher früher als später mit dem Thema IT-Sicherheit konfrontiert. IT-Infrastrukturen können hier bereits sehr komplex werden. Das Thema IT-Sicherheit im Bereich KMU wird daher oft aus Gründen des fehlenden Fachpersonals, des fehlenden Know-hows oder schlichtweg aufgrund des erforderlichen Finanzierungsaufwandes rudimentär behandelt. Dazu kommen neue Herausforderungen beim Aufbau von Netzwerken im Zuge der Digitalisierung und Industrie 4.0 sowie häufig auch der Einsatz von Cloud-Technologie.

Viele Unternehmen sind bereits Opfer eines Cyberangriffs gewesen und möchten im Rahmen des oft notwendigen Neuaufbaus der IT-Infrastruktur die Sicherheit verbessern. Der entstandene finanzielle Schaden, auch durch Verlust der Reputation bei Kunden, ist dabei meist um ein vielfaches höher, so dass sich präventives Vorgehen unter Einsatz der erforderlichen Ressourcen an dieser Stelle als durchaus sinnvoll darstellt. Zielstellung der Arbeit ist es, unter Berücksichtigung vorhandener Richtlinien zur Informationssicherheit, wie BSI IT-Grundschutz, ISO 27001 oder VdS 10000 für KMU, zielgerichtete Maßnahmen und Empfehlungen zu konzeptionieren, um ein zunächst vereinfachtes IT-Grundschutz-Profil zu entwickeln. Dieses soll bei Bedarf als Hilfestellung für weiterführende, individuelle Sicherheitskonzepte geeignet sein. Die Maßnahmen werden dabei möglichst praxisnah am Beispiel eines Referenzunternehmens beschrieben und berücksichtigen die Vorgehensweisen moderner Cyberangriffe. Maßnahmen im Rahmen des Datenschutzes (DSGVO) werden in dieser Arbeit nicht behandelt.

Abstract

In the previous seminar work on the subject of “Motivation and the Sequence of Cybercriminal Attacks in Manufacturing Companies”, the most important aspects and fundamentals for describing the initial problem were given. On the basis of the facts presented and the information taken from the press on the development of the general threat situation, it can be assumed that the probability of targeted attacks on every company is steadily increasing. Also, and above all, companies from the SME sector (small and medium-sized enterprises) are confronted with the issue of IT security sooner rather than later due to the increasing threat from cybercriminal attacks. IT infrastructures can already become very complex here. The subject of IT security in the SME sector is therefore often dealt with in a rudimentary manner due to the lack of IT specialist staff, the lack of know-how or simply because of the necessary financing costs. In addition, there are new challenges in setting up networks in the course of digitization and Industry 4.0 as well as increasing use of cloud technology.

Many companies have already been victims of a cyber-attack and want to improve security as part of the often necessary rebuilding of the IT infrastructure. The resulting financial damage, including the loss of reputation with customers, is usually many times higher, so that a preventive approach using the necessary resources makes sense at this point. The aim of this thesis is to conceptualize targeted measures and recommendations for SMEs considering existing guidelines for information security, such as BSI IT-Grundschutz, ISO 27001 or VdS 10000, in order to develop an underlying simplified IT basic protection profile. If necessary, this should be suitable as an aid for advanced, individual security concepts. The measures are described as practically as possible using the example of a reference company and considering the procedures of modern cyber-attacks. Measures regarding data protection (GDPR) are not dealt with in this work.

Inhaltsverzeichnis

1 EINLEITUNG	1
1.1 Aktuelle Lage der IT-Sicherheit bei KMU	1
1.2 Zielsetzung und Vorgehensweise	3
1.3 Begriffsdefinitionen und Abgrenzung	5
2 GRUNDLAGEN	7
2.1 Vorgaben und Richtlinien zur Informationssicherheit	7
2.1.1 BSI IT-Grundschutz	7
2.1.2 ISO/IEC Normreihe 2700x	8
2.1.3 ISIS 12 Methodik.....	9
2.1.4 VdS 10000/10020	11
2.1.5 Weitere Richtlinien und Empfehlungen	13
2.1.5.1 IEC 62443	13
2.1.5.2 IT-Sicherheitsgesetz.....	14
2.1.5.3 CIS-Controls.....	14
2.2 Referenzmodell eines KMU	16
2.2.1 Organisation	16
2.2.2 Netzwerk.....	17
2.2.3 Active Directory.....	19
2.2.4 Unternehmensanwendungen	21
2.2.5 Cloud-Anwendungen	22
2.2.6 Industrial-IT.....	22
2.2.7 Sicherheitssysteme.....	23
3 ORGANISATORISCHE MAßNAHMEN	26
3.1 Organisation der Informationssicherheit	27
3.1.1 Leitlinie und Strategie zur Informationssicherheit	27
3.1.2 Informationssicherheitsbeauftragter (ISB)	28
3.1.3 Organisationsstruktur	29
3.1.4 Einbeziehen der Mitarbeiter	31
3.2 Prozesse und Dokumentation.....	33
3.2.1 Identitätsmanagement (IAM).....	33
3.2.2 Inventarisierung und Dokumentation.....	35
4 TECHNISCHE SCHUTZMAßNAHMEN	37
4.1 Mehrstufiges Modell	37
4.2 Stufe 0 – Basisschutz.....	40

4.2.1 Zugangsschutz	40
4.2.1.1 Authentifizierung	40
4.2.1.2 Passwortsicherheit	42
4.2.1.3 Pass-the-Hash und Pass-the-Ticket	47
4.2.1.4 Privilegierte Konten	49
4.2.2 Active Directory Struktur	55
4.2.3 Applikationssicherheit	57
4.2.4 Patchmanagement	59
4.2.5 Protokollierung	61
4.2.6 Datensicherung und Notfallkonzepte	63
4.3 Stufe 1 – Perimeter	65
4.3.1 Firewall und DMZ	65
4.3.2 Web-Sicherheit	68
4.3.3 DNS-Sicherheit	69
4.3.4 E-Mail-Sicherheit	72
4.3.5 Intrusion Detection und Prevention (IDS/IPS)	74
4.4 Stufe 2 – Endpunkte	75
4.4.1 Anti-Virus	75
4.4.2 Firewall	78
4.4.3 Web-Filter	79
4.4.4 Detektion und Reaktion	80
4.4.5 Weitere Funktionen	81
4.5 Stufe 3 – Netzwerk	82
4.5.1 Segmentierung	82
4.5.2 Detektion und Reaktion	85
4.6 Weitere Überlegungen	89
4.6.1 Industrial-IT	89
4.6.2 Mobiles Arbeiten	91
4.6.3 Cloud-Technologien	93
5 FAZIT UND AUSBLICK	94
LITERATUR- UND QUELLENVERZEICHNIS	95
ABKÜRZUNGSVERZEICHNIS	104

Abbildungsverzeichnis

Abbildung 1 - Zunahme der Angriffe auf Unternehmen 2015 - 2019 [Bit20a], S. 7	2
Abbildung 2 - ISMS Lebenszyklus nach Deming [BSI17b]	6
Abbildung 3 - Übersicht über die ISO/IEC 27000 Normenreihe [Bun20]	9
Abbildung 4 - Das ISIS12 Vorgehensmodell [ITS20]	10
Abbildung 5 - Vergleich der Richtlinien in Anlehnung an [Fra14], S. 27 und [Gro19]	12
Abbildung 6 - Klassifizierung von Organisationen nach CIS-Controls [CIS21b], S. 5	15
Abbildung 7 - Vereinfachter Netzwerkplan der Firma Musterbau GmbH	17
Abbildung 8 - Übersicht Active Directory „musterbau.intern“	20
Abbildung 9 - Hemmnisse bei der Verbesserung der IT-Sicherheit KMU [WIK17], S. 76	29
Abbildung 10 - Struktur des mehrstufigen Schutzkonzeptes	39
Abbildung 11 - Beispiel für Credential Dumping mit Hilfe des Tools „Mimikatz“ [Wis21]	43
Abbildung 12 - Active Directory Verwaltungsebenen-Modell [Mic14], S. 16	51
Abbildung 13 - Idee eines Firewall-Systems [Poh19], S. 329	65
Abbildung 14 - MX- und SPF-Eintrag in der Domain „example.com“ [Sch20], S. 432	72
Abbildung 15 - Verhindern von Lateral Movement durch Netzwerksegmentierung [Sop20]	78