Nico Ohlig

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

Bachelorarbeit

GRIN

Bibliografische Information der Deutschen Nationalbibliothek:

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

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 Verlag

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 steigendenden 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

Abbildungsverzeichnis