

CertPro® PRESS
Professional Learning

Diese Broschüre zeigt in der Einführung den allgemeinen Trend in der Computertechnik auf. Zum besseren Verständnis werden zudem potentielle Gefahren verdeutlicht, die im Umgang mit mobilen Geräten, wie Smartphones, Tablet-Computern, aber auch dem Internet entstehen.

Um den Schutz gegen mögliche Angriffe auf diese Geräte, und somit auf die darauf gespeicherten Daten gewähren zu können, enthält diese Broschüre im hinteren Teil eine Übersicht möglicher, wirksamer Schutzmaßnahmen, die von Anwendern in der Praxis auch sofort umgesetzt werden können - ganz nach dem Motto: „**Gib Hackern keine Chance!**“.



SECURITY AWARENESS

Leitfaden zur IT-Sicherheit für Anwender

Inhalte

Seite

Aktuelle Trends und Entwicklungen 4

Aktuelle Gefahren und Angriffsmethoden.. 10

- Ransomware, Viren, Würmer, Trojaner & Co..... 12
- Social Engineering - Feinde unter uns... 24
- Physikalische Angriffe 30
- Phishing & Whaling - die Tricks der Angreifer 32
- Social Media Angriffe - Facebook, Twitter & Co. 40

Wirksame Schutzmaßnahmen

- Sicherer Umgang mit Daten..... 49
- Sicherer Umgang mit E-Mails 51
- Sicherer Umgang mit dem Internet..... 55
- Sicherer Umgang mit sozialen Netzwerken 57
- Sicherer Umgang mit Passwörtern 59
- Sicherer Arbeitsplatz..... 64



Aktuelle Trends und Entwicklungen

Die mobile Datenverarbeitung stellt seit Jahren bereits einen unaufhalt-samen Trend dar - Laptop- und Tablet-Computer, sowie moderne Smartphones ermöglichen es, prinzipiell an jedem Ort und zu jeder Zeit auf seine Daten, sowie auch auf das Internet zugreifen zu können...!



Viren, Würmer, Trojaner & Co.

Neben „Ransomware“ existieren noch weitere, teils ebenso gefährliche „Produkte“ der Angreifer: Viren, Würmer, Trojaner & Co.... - und einige derer ermöglichen den Angreifern das komplette „Fernsteuern“ von Computersystemen und Smartphones...

Trojaner & Rootkits - Die Macht der Angreifer



Trojaner bieten dem Angreifer oft die folgenden Funktionen:

- Remote-Zugriff
- Datenübertragung
- FTP-Server-Funktionalität
- Antivirus- und Firewall-Killer
- Webcam- und Desktop-Übertragung und -Aufzeichnung
- Sprachaufzeichnung
- Keylogger-Funktionalität
- Ausspähen von Kennwörtern
- Remote-Registry-Verwaltung

Rootkits dienen dem Angreifer zum „Tarnen und Verstecken“



Im Gegensatz zu Viren und Würmern bieten aktuelle Trojaner dem Angreifer eine Vielzahl an Funktionen und Möglichkeiten, die teilweise sogar in kostenpflichtigen Remoteverwaltungstools nicht enthalten sind.

„Shoulder Surfing“ - ohne großen Aufwand...

Hierbei schaut ein Angreifer dem Benutzer während des **Anmeldevorgangs** über die Schulter (deutsch: „**Schulter surfen**“), genauer: *auf die Tastatur*, um so an die **Anmeldedaten** wie den *Anmeldenamen* und das *Password* zu gelangen.



Beim „Shoulder Surfing“ kommen oft auch Spycams, versteckt und getarnt in Kugelschreibern, Schlüsselanhängern und ähnlichem zum Einsatz!

Phishing-URL - man sieht den Unterschied...

Originale URL	Beispiel für Phishing-URL
http://www.twitter.com	http://www.tvvitter.com („v v“ statt „w“)
http://www.apple.com	http://www.appel.com/-events/june-2016
http://www.yahoo.com	http://europe.yahoo.com/registration?.intl=de&.lang=de-DE&pd=pm_ver%253D0
http://www.amazon.de	http://www.arnazon.de
http://www.deutsche-bank.de	http://www.deutsche-bank.de.finanzeu.portal/IID=50850150&AID=IPSTANDARD&n=/onlinebanking
http://www.facebook.de	http://www.facebook.de.online-treff.de/beitrag/video/204935/
http://www.facebook.de	http://www.facebock.de/beitrag/31145



Die Beispiele für Phishing-URLs werden von Angreifern oft in E-Mails eingebaut, um nichtsahnende Benutzer zum Draufklicken zu verführen.

Sicherer Umgang mit Passwörtern...

Praxistipps für den sicheren Umgang mit Passwörtern

Beachten Sie die folgenden Regeln bei der Auswahl sicherer Passwörter:

- **mindestens** 8 Zeichen lang (gerne mehr);
- enthält **wenigstens** die folgenden Kategorien:
 - Großbuchstaben (A bis Z)
 - Kleinbuchstaben (a bis z)
 - Zahlen (0 bis 9)
 - Sonderzeichen (z. B.: !, #, @, %, usw.)
- beinhaltet **nicht** mehr als 3 aufeinander folgende Buchstaben, sowie auch **nicht** den Anmelde- oder vollständigen Namen.

Beispiel für ein „sicheres“ Passwort: **L{Ki3XG(\$jPz>GA&Ka4**



Ein Passwort sollte für Dritte niemals zugänglich sein. Man sollte das Passwort in einem bestimmten Zeitabstand unbedingt ändern, damit es durch Angreifer auf längere Sicht hin nicht einfach erraten werden kann.

Die Informationen in diesem Produkt werden ohne Rücksicht auf einen eventuellen Patentschutz veröffentlicht. Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt. Bei der Zusammenstellung von Texten und Abbildungen wurde mit größter Sorgfalt vorgegangen. Trotzdem können Fehler nicht vollständig ausgeschlossen werden. Verlag, Herausgeber und Autoren können für fehlerhafte Angaben und deren Folgen weder eine juristische Verantwortung noch irgendeine Haftung übernehmen.

Alle Rechte vorbehalten, auch die der fotomechanischen Wiedergabe und der Speicherung in elektronischen Medien.

Fast alle Hard- und Softwarebezeichnungen und weitere Stichworte und sonstige Angaben, die in diesem Buch verwendet werden, sind als eingetragene Marken geschützt. Da es nicht möglich ist, in alle Fällen zeitnah zu ermitteln, ob ein Markenschutz besteht, wird das ®-Symbol in diesem Buch nicht verwendet.

Print-Ausgabe: ISBN 978-3-9447-4909-9

ebook-Ausgabe: ISBN 978-3-9447-4910-5

Copyright © 2016 by CertPro Press-Verlag,
ein Imprint der CertPro® Limited, Im Pflänzer 14, 55545 Bad Kreuznach/Germany.
Alle Rechte vorbehalten.

Autor: Carlo Westbrook

Herstellung: CertPro® Limited

Druck und Verarbeitung: WIRmachenDRUCK GmbH, Mühlbachstr. 7, 71522 Backnang/Deutschland

ebook-Distribution: libreka! GmbH, Frankfurt am Main

Printed in Germany

