Zertifikatsprogramm - Z213

Netzwerkhacking

- Bedrohungen der IT-Sicherheit
- Grundlagen von Hacking-Techniken
- IT-Verteidigungsmaßnahmen
- Penetration Testing
- Fallbeispiele zur Behandlung von netzwerkzentrierten Angriffen

Prof. Dr. Martin Rieger
Patrick Eisoldt, M.Eng.
David Schlichtenberger, M.Sc.
Benjamin Welte, M.Eng.
Michael Kotzjan, B.Sc.
Patrick Geiger

Open C³S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

Prof. Dr. Martin Rieger
rieger@hs-albsig.de
+49 (0) 07571 / 732 - 9124

Benjamin Welte, M.Eng.
welte@hs-albsig.de
+49 (0) 07571 / 732 - 9554

Netzwerk – Missbrauch – Hacking

Studienbrief 1: Bedrohungen der IT-Sicherheit

Studienbrief 2: Grundlagen von Hacking-Techniken

Studienbrief 3: IT-Verteidigungsmaßnahmen

Studienbrief 4: Penetration Testing

Studienbrief 5: Fallbeispiele zur Behandlung von netzwerkzentrierten Angriffen

---

Autoren:

Prof. Dr. Martin Rieger

Patrick Eisoldt, M.Eng.

David Schlichtenberger, M.Sc.

Benjamin Welte, M.Eng.

Christian Schneider, M.Eng.

Michael Kotzjan, B.Sc.

Patrick Geiger

---

2. Auflage

Hochschule Albstadt-Sigmaringen

Institut für wissenschaftliche Weiterbildung
Open C^{3}S | Zertifikatsprogramm
Gartenstraße 15
72458 Albstadt

2. Auflage (2021-09-03)

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Merksatz	M
Quelltext	Q

II. Zu den Autoren

Prof. Dr. Martin Rieger studierte Elektro- und Informationstechnik an der Technischen Universität München und schloss an derselben Hochschule die Promotion mit Auszeichnung ab. Ein Schwerpunkt seiner Forschungsarbeit lag in der Erstellung von Methoden und Werkzeugen zur Modellierung sowie Analyse und Optimierung elektrischer Schaltungen. Er war fünf Jahre Leiter des Labors für schnelle Analog-ICs in der IC-Entwicklungsabteilung des Forschungs- und Entwicklungszentrums der Firma Thomson Multimedia in Villingen. In der Zeit bei Thomson Multimedia war er Erfinder bzw. Miterfinder an 15 deutschen, 12 europäischen und 8 weltweiten Patenten.

Seit 1993 ist er als Professor an der Fakultät Engineering der Hochschule Albstadt-Sigmaringen auf den Gebieten Informatik und Informationstechnik tätig. Im Labor für Eingebettete Systeme und IT-Sicherheit betreibt er anwendungsnahe Forschung auf den Gebieten Embedded Systems und IT-Sicherheit. Er hatte über viele Jahre an der Hochschule Albstadt-Sigmaringen Positionen als Studiendekan, Prodekan, Prorektor und Rechenzentrumsleiter inne.

Prof. Dr. Rieger ist Initiator und Gründungs-Studiendekan des Master-Studiengangs Digitale Forensik, der in Kooperation mit der Friedrich-Alexander Universität Erlangen-Nürnberg und der Ludwig-Maximilians-Universität München betrieben wird.

Er leitet das vom BMBF geförderte Zertifikatsprogramm Open-C^3S, das 35 Hochschul-Zertifikatsmodule auf dem Gebiet Cybersicherheit anbietet und das kooperativ von der Hochschule Albstadt-Sigmaringen, der Friedrich-Alexander-Universität Erlangen-Nürnberg, der Freien Universität Berlin, und der Ludwig-Maximilians-Universität München, getragen wird.

Patrick Eisoldt, M. Eng. hat an der Hochschule Albstadt-Sigmaringen und der Glyndŵr University in Wales studiert. 2012 schloss er erfolgreich sein Masterstudium Systems Engineering ab. Im Rahmen seiner Master-Thesis konzipierte und realisierte er einen prototypischen Editor zur Projektierung von Prozessleitsystemen der Firma Siemens nach dem Ursache-Wirkung-Prinzip. Von November 2010 bis August 2011 unterstützte er das Institut für Wissenschaftliche Weiterbildung bei der Erstellung von Studienbriefen für den Studiengang Digitale Forensik.

Seit 2012 ist er für das Open Competence Center for Cyber Security als Modulentwickler tätig.

David Schlichtenberger studierte Medien- und Kommunikationsinformatik an der Hochschule Reutlingen. Nach seinem Masterstudium arbeitete er einige Jahre als Webentwickler und Kundenberater für Internetservices. Seit November 2014 ist er als akademischer Mitarbeiter an der Hochschule Albstadt-Sigmaringen am Institut für Wissenschaftliche Weiterbildung beschäftigt.

Benjamin Welte absolvierte den Bachelor-Studiengang Kommunikations- und Softwaretechnik an der Hochschule Albstadt-Sigmaringen.
Während des Bachelors arbeitete er als Werkstudent im Bereich der Softwareentwicklung.
Seit Februar 2016 arbeitet er als Modulentwickler und Tutor im Zertifikatsprogramm des Open Competence Center for Cyber Security. Innerhalb dieser Zeit absolvierte er ebenfalls den Master-Studiengang Systems Engineering an der Hochschule Albstadt-Sigmaringen.

Christian Schneider hat an der Hochschule Albstadt-Sigmaringen Systems Engineering studiert. Während seines Bachelorstudiums arbeitete er für einen Antivirenhersteller und als Webentwickler. Weiter betreute er, im Rahmen von Vorlesungen, Studenten als Tutor.
Von 2016 bis 2017 unterstützte er als wissenschaftlicher Mitarbeiter das Institut für wissenschaftliche Weiterbildung bei der Erstellung von Studienbriefen.

Michael Kotzjan studierte Allgemeine Informatik an der Hochschule Furtwangen. Während seines Bachelorstudiums arbeitete er als Softwaretester im Bereich der Medizintechnik und betreute als Tutor Studenten im Rahmen von Vorlesungen.
Seit 2019 absolviert er den Master-Studiengang Systems Engineering und unterstützt als wissenschaftlicher Mitarbeiter das Institut für wissenschaftliche Weiterbildung bei der Erstellung von Studienbriefen.

Patrick Geiger studiert IT-Security an der Hochschule Albstadt-Sigmaringen. Während des Studiums unterstützte er als studentische Hilfskraft das Zertifikatsprogramm in den Modulen der digitalen Forensik. Seit März 2019 arbeitet er am Institut für wissenschaftliche Weiterbildung an Studienbriefen und Modulentwicklungen mit.

III. Modullehrziele

Dieses Modul soll zeigen, wie einfach es in vielen Fällen ist, einen Angriff durchzuführen. Wir wollen vermitteln, worauf ein erfolgreicher Angriff basiert:

- Ansatz des Angriffs
- Mechanismen von Schadsoftware
- Stufenweises Vorgehen
- Schadsoftware tarnt sich
- Schadsoftware verankert sich im System
- Schadsoftware ist „fernsteuerbar“

Es soll auch gezeigt werden, wie vorgegangen werden kann, wenn ein Angriff bereits eingetreten ist oder eventuell sogar noch aktiv ist.

- Incident Response, „Feuerwehr“
- Forensische Ermittlungen

Die bekannten Prinzipien zum Aufbau sicherer digitaler Infrastruktur werden erlernt:

- Bausteine sicherer digitaler Netze: Zutrittskontrolle, Zugriffskontrolle, Verschlüsselung, Firewalls
- Analyse und Design der erforderlichen Sicherheitsmaßnahmen
- Schutzmaßnahmen für Clients
- Konzepte zur Netzwerksicherheit

Wir lernen den Nutzen einer ständigen Überwachung der Netzwerksicherheit kennen:

- Network Security Monitoring
- Vorgänge erfassen
- Vorgänge detektieren
- Vorgänge analysieren

Es ist sinnvoll, Systeme selbst zu testen (Penetrationstests) und somit bereits möglichst früh einen Großteil der Schadsoftware auszusperren.

- Schließen der Sicherheitslücken
- Schulung der Mitarbeiter

Studienbrief 1 Bedrohungen der IT-Sicherheit

1.1 Lernziele

Zunächst sollen wichtige Begriffe im Umfeld der IT-Sicherheit und der IT-Angriffe vorgestellt werden, damit sich der Leser in diesen Begrifflichkeiten ausdrücken kann. Dann wird in Beispielen gezeigt, wie einfach es in vielen Fällen ist, einen Angriff durchzuführen. Wir wollen vermitteln, worauf ein systematisch geplanter und durchgeführter Angriff basiert.

- Ansatz des Angriffs
- Mechanismen von Schadsoftware
- Stufenweises Vorgehen
  - Schadsoftware tarnt sich
  - Schadsoftware verankert sich im System
  - Schadsoftware ist „fernsteuerbar“

1.2 Schwachstellen, Bedrohungen und Angriffe

Definition 1.1: Schwachstelle; Verwundbarkeit

Unter einer Schwachstelle (engl. *weakness*) verstehen wir eine Schwäche eines Systems oder einen Punkt, an dem das System verwundbar werden kann. Eine Verwundbarkeit (engl. *vulnerability*) ist eine Schwachstelle, über die die Sicherheitsdienste des Systems umgangen, getäuscht oder unautorisiert modifiziert werden können.

D

Beispielsweise zählt die Diebstahlgefahr zu den physischen Schwachstellen mobiler Geräte. Weitere Schwachstellen können durch die unsachgemäße Nutzung des Systems, durch Softwarefehler oder auch durch unsichere Kommunikationsverbindungen entstehen. Typische softwarebedingte Schwachstellen, die häufig zu einer Verwundbarkeit werden, sind Programme, in denen aufgrund einer fehlenden Eingabeüberprüfung Pufferbereichsüberläufe nicht korrekt abgefangen werden.

Definition 1.2: Bedrohung

Eine Bedrohung (engl. *threat*) des Systems zielt darauf ab, eine oder mehrere Schwachstellen oder Verwundbarkeiten auszunutzen, um einen Verlust der Datenintegrität, der Informationsvertraulichkeit oder der Verfügbarkeit zu erreichen oder um die Authentizität von Subjekten zu gefährden.

D

Unter dem Risiko (engl. *risk*) einer Bedrohung verstehen wir die Wahrscheinlichkeit (oder relative Häufigkeit) des Eintritts eines Schadensereignisses, verknüpft mit der dadurch hervorgerufenen Höhe des potentiellen Schadens. Hier verstehen wir Risiko als Produkt aus Schaden und Wahrscheinlichkeit. Also:

Risiko

Definition 1.3: Risiko

$$Risiko = Schaden * Wahrscheinlichkeit$$

D

Studienbrief 2 Grundlagen von Hacking-Techniken

2.1 Schadsoftware

Spezielle Klassen von Bedrohungen eines IT-Systems gehen von Viren, Würmern und Trojanischen Pferden aus, die wir als Schadsoftware (engl. *malware* oder *malicious code*) bezeichnen. Es handelt sich hierbei um Programme, die festgelegte, dem Benutzer jedoch verborgene, Funktionen ausführen. Die Festlegung der zusätzlichen und beabsichtigten (i. d. R. böswilligen) Funktionalität unterscheidet diese Klasse von Programmen von den so genannten Wanzen (engl. *bugs*), deren Fehlverhalten meist von nicht beabsichtigten Programmierfehlern verursacht wird.

Im Folgenden finden Sie eine Auflistung möglicher Architektur-Schwächen von Software:

Architektur-Schwächen

- Die gemeinschaftliche Nutzung von Programmen und Daten (engl. *sharing*). Eine solche gemeinsame Nutzung wird u. a. über eine zum Teil sehr freizügige Netzwerkfreigabe oder über öffentliche Verzeichnisse ermöglicht.
- Eine weitere wesentliche Eigenschaft ist die *universelle Interpretierbarkeit* von Daten. Sie besagt, dass kein Unterschied zwischen Daten und Programmen besteht. Programme können demnach wie Daten leicht modifiziert werden, indem man sie beispielsweise um einen Schadensteil erweitert.
- Als dritte wesentliche Eigenschaft ist die Transitivität des Informationsflusses zu nennen. Falls eine Information vom Rechner A zum Rechner B fließt und es Möglichkeiten gibt, Informationen von B zu einem Rechner C fließen zu lassen, so kann die Information auch von A zu C weitergeleitet werden. Die Transitivität wird insbesondere von Würmern ausgenutzt, um sich auf diese Weise zu verbreiten.

Techniken zur Bedrohungsabwehr

Zur Abwehr der Bedrohungen kann man drei Ansätze verfolgen, die in der Praxis in verschiedenen Kombinationen eingesetzt werden:

- Techniken zur Verhinderung (engl. *prevention*) von Angriffen wie beispielsweise die Verwendung stark typisierter Programmiersprachen, Code-Verifikation oder die Beschränkung von Zugriffen aufgrund von systembestimmten Regeln.
- Die zweite Klasse von Ansätzen beschäftigt sich mit Techniken zur Erkennung und frühzeitigen Abwehr möglicher Bedrohungen. Als Beispiele seien statische Analysen des Programmcodes genannt, um z. B. Code-Stücke, die eine Buffer-Overflow-Schwachstelle aufweisen (u. a. Kopieren von Zeichenfolgen ohne die Längenangaben zu prüfen), zu identifizieren und zu korrigieren. Aber auch die bekannten Viren-Scanner und Intrusion Detection Systeme gehören in diese Klasse von Techniken, die anhand charakteristischer Merkmale versuchen, potentielle Schadsoftware zu erkennen.
- Zu der dritten Klasse von Ansätzen zählen Techniken, die darauf abzielen, die Auswirkungen von eingetretenen Bedrohungen zu begrenzen (engl. *mitigation*). Dazu zählen Isolierungsansätze wie das Sandboxing, die darauf abzielen, Anwendungsbereiche gegeneinander abzuschotten, so dass ein Schaden, der bei der Ausführung eines Anwendungsprogramms auftritt, sich nicht auf andere Anwendungsbereiche ausbreiten und womöglich das ganze System beeinträchtigen kann.

Studienbrief 3 IT-Verteidigungsmaßnahmen

3.1 Prinzipien und grundlegende Mechanismen

D

Definition 3.1: Security Engineering

„Beim Security Engineering geht es um die Entwicklung sicherer Systeme, die auch im Fehlerfall, durch Missgeschicke oder Böswilligkeit, zuverlässig bleiben. Security Engineering adressiert Werkzeuge, Prozesse und Methoden für den Entwurf, die Implementationen, den Test von IT-Systemen und zur Adaption des Systems, falls in der Systemumgebung Änderungen auftreten.“ (frei übersetzt nach [Anderson, 2008] S.3)

Security Engineering ist ein Teilbereich der Ingenieurswissenschaften, welcher darauf abzielt, bereits ab der Entwurfsphase, anhand von bewährten Prinzipien und Mechanismen, sichere und robuste IT-Systeme zu entwickeln. Bei der Entwicklung von komplexer Software sind zahlreiche Akteure involviert, die jeweils eine unterschiedliche Sichtweise auf das IT-System haben. Über Security Engineering wird versucht, diese Akteure in einen sicheren Entwicklungsprozess mit einzubeziehen, um in IT-sicherheitsrelevanten Aspekten die richtigen Entscheidungen zu treffen. Insbesondere durch die stetig wachsende Geschwindigkeit in der neue IT-Systeme entwickelt werden (vgl. auch Agile Softwareentwicklung [Baca and Carlsson, 2011]) und durch Erstellung von Gesamtsystemen aus modularisierten Teilen, ist das Risiko, sicherheitsrelevante Aspekte zu vernachlässigen, vorhanden.

Die wichtigsten Prinzipien des Security Engineering sind das

- Erlaubnisprinzip
- Vollständigkeitsprinzip
- Need-to-know-Prinzip
- Prinzip der Benutzerakzeptanz

Das Erlaubnisprinzip (engl. *fail-safe defaults*) fordert, dass grundsätzlich jeder Zugriff verboten ist (default deny) und nur durch eine explizite Erlaubnis ein Zugriffsrecht gewährt werden kann.

Das Vollständigkeitsprinzip (engl. *complete mediation*) besagt, dass jeder Zugriff auf seine Zulässigkeit zu prüfen ist. Ein System, in dem Zugriffsrechte zur Nutzung von Dateien vergeben werden und eine Rechteüberprüfung nur beim Öffnen einer Datei durchgeführt wird, erfüllt beispielsweise nicht das Vollständigkeitsprinzip. In solchen Systemen ist es möglich, dass ein Benutzer eine Datei über lange Zeiträume geöffnet hält und damit das Zugriffsrecht darauf nutzt, obwohl der Besitzer der Datei zwischenzeitlich dem Benutzer dieses Recht bereits wieder entzogen haben kann.

Das Prinzip der minimalen Rechte (engl. *need-to-know*) fordert, dass jedes Subjekt nur genau die Zugriffsrechte erhalten darf, die es zur Erfüllung seiner Aufgaben benötigt. Systeme, in denen ein Superuser unbeschränkte Rechte besitzt, sind ein offensichtliches Beispiel für die Nicht-Einhaltung des Need-to-know Prinzips.

Prinzip der Benutzerakzeptanz

Das Prinzip der Benutzerakzeptanz (engl. *economy of mechanism*) fordert, dass die eingesetzten Sicherheitsmechanismen einfach zu nutzen sein müssen und dass sie automatisch und routinemäßig angewendet werden.

Studienbrief 4 Penetration Testing

4.1 Methodik für die Durchführung von Pentrationstests

5 Phasen Methodik

In diesem Kapitel wird eine in fünf Phasen gegliederte Methodik zur Durchführung von Penetrationstests vorgestellt. Diese Methodik berücksichtigt die bisher diskutierten Aspekte und wurde im Hinblick auf eine möglichst große Allgemeingültigkeit entwickelt. Zentraler Bestandteil der Methodik ist eine strukturierte Vorgehensweise zur Durchführung von Penetrationstests, auf dessen Basis individuelle Ablaufpläne für konkrete Penetrationstests gebildet werden können.

Anforderungen an eine Methodik für die Durchführung von Penetrationstests

Die Methodik beschreibt und strukturiert die Durchführung eines Penetrationstests im Auftrag. Daher muss immer wieder eine Orientierung auf die Ziele des Auftraggebers erfolgen bzw. Sorge getragen werden, dass diese Orientierung nicht außer Acht gelassen wird.

Dies bedeutet beispielsweise, dass die zur Erreichung der Ziele notwendigen Prüfungsschritte beschrieben werden, bzw. dass erläutert wird, ob die Ziele überhaupt sinnvoll mit einem Penetrationstests erreicht werden können. Des Weiteren müssen Maßnahmen zur Einhaltung der rechtlichen Bestimmungen (zur Beachtung von organisatorischen bzw. personellen Voraussetzungen) für die Durchführung von Penetrationstests enthalten sein.

Darüber hinaus sollte eine Methodik zur Durchführung von Penetrationstests die nur begrenzt zur Verfügung stehende Zeit berücksichtigen und muss daher eine Bewertung des potenziellen Risikos bzw. einen Kosten/Nutzen Vergleich enthalten.

Prüfmodelle

Für die Gruppierung der einzelnen Prüfungsschritte empfiehlt sich ein modulorientierter Ansatz, wie z. B. der des OSSTMMs[1]. Dieser erlaubt eine thematische Gruppierung der durchzuführenden Schritte innerhalb eines Penetrationstests. Dies dient zum einen der Übersichtlichkeit, zum anderen kann so durch die Auswahl bzw. das Auslassen von bestimmten Modulen ein angemessener Penetrationstest zusammengestellt werden.

Im Rahmen eines konkreten Penetrationstests können aus wirtschaftlichen Gründen oftmals nicht alle möglichen Prüfungsmodule bearbeitet werden. Dies würde zwar eine vollständige Prüfung sicherstellen, aber auch zu einem hohen zeitlichen Aufwand führen, der u. U. nicht mit den Zielen des Auftraggebers vereinbar bzw. nicht den konkreten Sicherheitsanforderungen angemessen ist. Bei sehr hohen Sicherheitsanforderungen sollte ein möglichst vollständiger Test durchgeführt werden. D. h., dass alle bzw. die meisten Module angewendet werden müssen und dass alle Systeme des Auftraggebers mit in den Test eingeschlossen werden. Bei niedrigen Sicherheitsanforderungen können hingegen bestimmte Module ausgelassen werden und/oder nur exponierte bzw. von „außen“ sichtbare Systeme geprüft werden. Der Umfang des Penetrationstests sollte dabei durch wirtschaftliche Überlegungen bestimmt werden. Es gilt die Kosten bzw. Risiken der Prüfungstätigkeiten mit den möglichen Kosten bzw. Risiken, die durch einen Angriff entstehen könnten, abzuwägen.

[1] OSSTMM = Open Source Security Testing Methodology Manual, z. B. `https://scadahacker.com/library/Documents/Assessment_Guidance/OSSTMM-3.0.pdf` [Stand: 15.08.2021]

Studienbrief 5 Fallbeispiele zur Behandlung von netzwerkzentrierten Angriffen

5.1 Herangehensweise in Beispielen

5.1.1 Vorfallsbehandlung eines Ransomware-Angriffs

Eine Ransomware ist ein Computer-Virus, der Dateien im Dateisystem oder den gesamten Client verschlüsselt und erst gegen Zahlung eines Lösegelds die Dateien wieder entschlüsselt. GandCrab ist eine solche Ransomware die seit dem Jahr 2018 in verschiedenen Varianten bis heute auftritt. Sie galt als eine der höchsten IT-Sicherheitsbedrohungen im Jahr 2018[1] [2].

Der Security Incident Prozess nach NIST besteht aus mehreren Phasen, wie in Studienbrief 3 ausführlich beschrieben. Wie in Abb. 5.1 zu sehen ist, sind dies die Phasen Preparation, Detection & Analysis, Containment Eradication & Recovery und Post-Incident Activity. Diese Vorgehensmodell wir nun für die Vorfallsbehandlung eines GrandCrab-Angriffs angelegt.

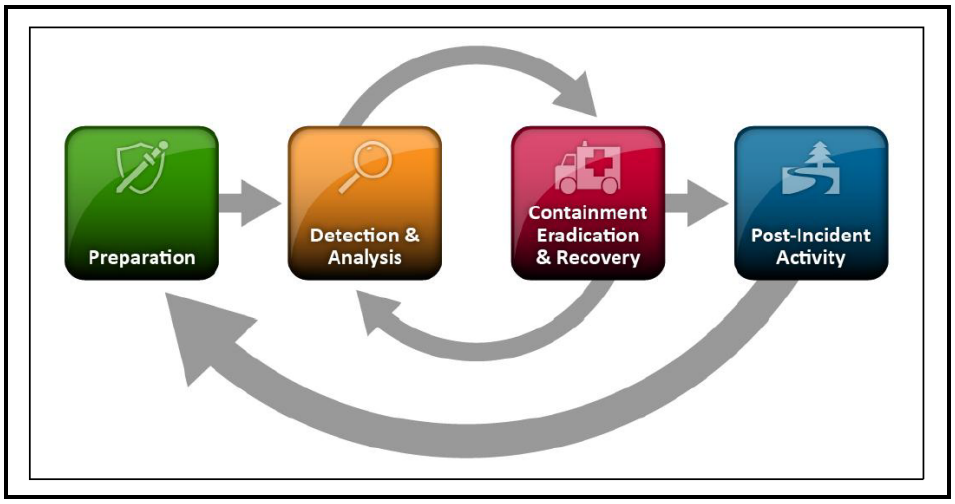

Abb. 5.1: Incident Response Life Cycle

Funktionsweise von GrandCrab

Die Ransomware GandCrab trat erstmals im Januar 2018 auf. Über das Jahr hinweg bis Anfang 2019 wurde GandCrab von den Angreifern immer wieder Weiterentwickelt, sodass imVerlauf verschiedene Versionen der Ransomware zum Vorschein traten. Das Konzept von GandCrab hat sich während seiner Entwicklung nicht grundlegend verändert. Auf Grund seiner Funktionalität zielt GandCrab ausschließlich auf Benutzer mit einem Windows Betriebssystem ab.

Zur Ausbreitung verwendet GandCrab verschiedene Wege. Bei den Verbreitungsarten gehört der Versand von Phishing-Mails zu den häufigsten Methoden. Hier wird GandCrab in einer Bewerbung versteckt und als ausführbare Datei übertragen. Es kommt auch vor, dass GandCrab als Makro-Virus in Word-Dokumenten im Anhang von E-Mails versandt wird. Dies kann ebenfalls als Bewerbung aber auch als Rechnung getarnt sein. Das CERT-Bund hatte eine Warnmeldung veröffentlicht, in welcher auf die Gefahren von GandCrab und den Angriffsvektor via E-Mail hingewiesen wurde. Die Angreifer nutzen für den Versand der E-Mails Bots um eine

[1] GandCrab Ransomware (2018): Gandcrab Ransomware Attack `https://www.securonix.com/web/wp-content/uploads/2018/07/Securonix-Threat-Research-GandCrab-Ransomware-Attack.pdf` [Stand: 15.08.2021]

[2] Hausarbeit Simon Eicker (2019), Digitale Forensik

Verzeichnisse

I. Abbildungen

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

VI. Tabellen

VII. Literatur

Allen, Malcom. Social Engineering: A Means To Violate A Computer System, 2006. https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-means-violate-computer-system-529.

Ross Anderson. *Security engineering*. John Wiley & Sons, 2008.

Dejan Baca and Bengt Carlsson. Agile development with security engineering activities. In *Proceedings of the 2011 International Conference on Software and Systems Process*, ICSSP '11, pages 149–158, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0730-7. doi: 10.1145/1987875.1987900. URL http://doi.acm.org/10.1145/1987875.1987900.

Bernhard C. Witt. Grundlagen des Datenschutzes und der IT-Sicherheit, 2017. https://www.uni-ulm.de/fileadmin/website_uni_ulm/iui/datenschutz/Loesung2017-07-17.pdf.

D. J. Bernstein. Syn cookies, 1996. http://cr.yp.to/syncookies.html.

BSI - Bundesamt für Sicherheit in der Informationstechnik. Konzeption von Sicherheitsgateways - der richtige Aufbau und die passenden Module für ein sicheres Netz, 2005.

BSI - Bundesamt für Sicherheit in der Informationstechnik. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz , 2012a. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Auditierungsschema.pdf?__blob=publicationFile".

BSI - Bundesamt für Sicherheit in der Informationstechnik. Zertifizierte IT-Sicherheit, 2012b. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Zertifizierte-IT-Sicherheit.pdf?__blob=publicationFile".

BSI - Bundesamt für Sicherheit in der Informationstechnik. *Sichere Nutzung von PCs unter Microsoft Windows 7*. 2013. https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Publikationen/BSI-E-CS_001.pdf?__blob=publicationFile".

BSI - Bundesamt für Sicherheit in der Informationstechnik. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, 2014. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema.pdf?__blob=publicationFile".

BSI (Bundesamt für Sicherheit in der Informationstechnologie. Die Lage der IT-Sicherheit in Deutschland 2015, 2015. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.pdf.

BSI (Bundesamt für Sicherheit in der Informationstechnologie). Ransomware, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf?__blob=publicationFile&v=2.

Open C³S
Open Competence Center for Cyber Security

Fort- und Weiterbildung

Neue Bedrohungszenarien stellen Sicherheitsexperten und IT-Verantwortliche in Unternehmen und einschlägigen Behörden vor immer größere Herausforderungen. Neue Technologien und Anwendungen erfordern zusätzliches Know-how und personelle Ressourcen.

Zur Erhöhung des Fachkräftepools und um neues Forschungswissen schnell in die Praxis zu integrieren, haben sich die im Bereich lehrenden und forschenden Verbundpartner zum Ziel gesetzt, ein hochschuloffenes transdisziplinäres Weiterbildungsprogramm im Sektor Cyber Security zu entwickeln. Auf der Grundlage kooperativer Strukturen werden wissenschaftliche Weiterbildungsmodule im Verbund zu hochschulübergreifenden Modulpaketen und abschlussorientierten Ausbildungslinien konzipiert und im laufenden Studienbetrieb empirisch getestet.

Die Initiative soll High Potentials mit und ohne formale Hochschulzugangsberechtigung über innovative Weiterbildungsangebote (vom Zertifikat bis zum Masterprogramm) zu Sicherheitsexperten aus- und fortbilden. Hierzu werden innovative sektorale Lösungen zur Optimierung der Durchlässigkeit von berulicher und hoch- schulischer Bildung entwickelt und für eine erfolgreiche Implementierung vorbereitet. Unter prominenter Beteiligung einschlägiger Verbände, der Industrie sowie Sicherheits und Ermittlungsbehörden verfolgt die Initiative das Ziel, im deutschsprachigen Raum eine Generation von Fachkräften wissenschaftlich aus- und weiterzubilden, die unser Internet schützen kann.

Open Competence Center for Cyber Security

Open C³S ist aus dem Verbundvorhabens Open Competence Center for Cyber Security entstanden. Das Gesamtziel des Programms war die Entwicklung eines hochschuloffenen transdisziplinären Programms wissenschaftlicher Weiterbildung im Sektor Cyber Security. Das Bundesministerium für Bildung und Forschung (BMBF) fördert das Großprojekt im Rahmen des Wettbewerbs „Aufstieg durch Bildung: offene Hochschulen“, der aus BMBF-Mitteln und dem Europäischen Sozialfonds finanziert wird.

Neun in Forschung und Lehre renommierte Hochschulen und Universitäten aus dem gesamten Bundesgebiet haben sich zum Ziel gesetzt, Online-Studiengänge auf dem Gebiet der Cybersicherheit zu entwickeln. Dieses Konzept soll den Studierenden ermöglichen, sich berufsbegleitend auf hohem Niveau wissenschaftliche Qualifikationen anzueignen und akademische Abschlüsse zu erlangen. Beruflich erworbene Kompetenzen können eingebracht werden. Die Bezeichnung „Open“ steht auch für die Öffnung des Zugangs zu akademischer Bildung ohne klassischen Hochschulzugang.

Mission der Initiative ist es, dringend benötigte Sicherheitsexperten aus- und fortzubilden, um mit einer sicheren IT-Infrastruktur die Informationsgesellschaft in Deutschland und darüber hinaus zu stärken.

Umsetzungsnahes Wissen ist ein wesentlicher Schlüssel um der wachsenden digitalen Bedrohung zu begegnen. Solange wir nicht in der Lage sind, Systeme hinreichend zu härten, Netzwerke sicher zu designen und Software sicher zu entwickeln, bleiben wir anfällig für kriminelle Aktivitäten. Unser Ziel ist es, die Mitarbeiter von heute zu Sicherheitsexperten und Führungskräften von morgen auszubilden und dafür zu sorgen, dass sich die Zahl und die Fertigkeiten dieser Experten nachhaltig erhöht.

Weitere Informationen zu Open C³S: https://open-c3s.de

Z213 Netzwerkhacking

Dieses Modul soll zeigen, wie einfach es in vielen Fällen ist, einen Angriff durchzuführen. Den Teilnehmenden wird vermittelt, worauf ein erfolgreicher Angriff basiert. Dabei wird auf den Ansatz des Angriffs und die Mechanismen von Schadsoftware eingegangen. Den Teilneh-menden wird das stufenweise Vorgehen der Schadsoftware vermittelt.

Es wird zudem aufgezeigt, wie vorgegangen werden kann, wenn ein Angriff bereits eingetre-ten oder eventuell sogar noch aktiv ist. Hierzu werden die Themen „Incident Response“ als, „Feuerwehr“ und die forensischen Ermittlungen näher eingegangen.

Mithilfe des Studienbriefs lernen die Teilnehmenden die bekannten Prinzipien zum Aufbau sicherer digitaler Infrastruktur kennen. Hier werden die einzelnen Bausteine der Netze, die Analyse und das Design der erforderlichen Sicherheitsmaßnahmen, aber auch die Schutz-maßnahmen für Clients sowie die Konzepte zur Netzwerksicherheit, eingehend betrachtet.

Die Teilnehmenden lernen den Nutzen einer ständigen Überwachung der Netzwerksicher-heit kennen, zu dem das Network Security Monitoring, die Erfassung und Detektierung so-wie die Analyse der Vorgänge gehören.

Es ist sinnvoll, Systeme selbst zu testen (Penetrationstests) und somit bereits möglichst früh einen Großteil der Schadsoftware auszusperren. Deshalb wird im Studienbrief auf die Schließung der Sicherheitslücken sowie die Schulung der Mitarbeiter eingegangen.