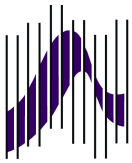
Hochschule
Ravensburg-Weingarten



Hochschule
Ravensburg-Weingarten
Technik | Wirtschaft | Sozialwesen

Erstellung eines Tools zur automatisierten Informationsbeschaffung von personenbezogenen Daten in Verbindung mit einem automatisierten Phishing-Mailgenerators

Bachelorarbeit

Social Engineering

im Studiengang Angewandte Informatik

an der Hochschule Ravensburg - Weingarten

von

Marco Lang Matr.-Nr.: 27416

Abgabedatum : 18. Januar 2019

Erklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit mit dem Titel

Generierung eines personalisierten Mail-Generators

selbststandig angefertigt, nicht anderweitig zu Pruefungszwecken vorgelegt, keine anderen als die angegebenen Hilfsmittel benutzt und woertliche sowie sinngemaesse Zitate als solche gekennzeichnet habe.

Weingarten, 18. Januar 2019

Autor Name

_____

Inhaltsverzeichnis

Kurzfassung

Abstract

Danksagung

Vorwort

1 Einleitung

1.1 Motivation

Laut dem Bundeskriminalamt hat sich die Zahl der Cyberkriminalität mit einem klaren Trend nach oben entwickelt. [Bun18] Aus diesem Grund werden System immer sicherer und Firewalls immer noch besser. Dadurch weichen Angreifer auf Methoden aus, bei denen der Mensch als Schwachstelle des Systems ausgenutzt wird. Eine häufig verwendetet Technik von Cyberkriminalität ist daher das E-Mail-Phishing.
In den neusten Fällen von Phishing-Attacken zeigt die Verbraucherzentrale Nordrhein-Westfalen, dass diese meist direkt an eine Person adressiert sind. Das heißt, in diesen Mails wird Information über die Opferperson verwendet. Ein Beispiel dafür, sind die gefälschten DSGVO-E-Mails, bei denen Persoen im Namen der Sparkasse, persönlich mit Namen angesprochen werden. [NW18]
Solch ein Angriff benötigt im Voraus eine ausführliche Recherche über die Zielperson. Die dadurch gewonnenen Daten über das Opfer, werden später für den Phishing-Mail-Angriff missbraucht.
Als Informationsquelle für die Recherche können beliebig viele Quellen verwendet werden. Jedoch ist in der heutigen Zeit das Internet eine der meistgenutzten Informationsquellen. [All18] Aus diesem Grund, wird im Rahmen dieser Abschlussarbeit gezeigt, wie eine automatisierte Suche nach personenbezogenen Daten im Internet aussehen kann und wie diese Daten für einen Phishing-Mail-Angriff verwendet werden können.

1.2 Zielsetzung

Ziel ist ein Programm zu entwickeln, welches automatisiert nach personenbezogenen Daten im Internet sucht und daraus eine Phishing-Mail generiert. Dabei soll das Programm zwei verschiedene Suchfunktionen haben.

Ziel 1 *Informationen zu einer bestimmten Person im Internet suchen.*

Die erste Suchfunktion beinhaltet die Suche nach Informationen einer bestimmten Person. Dadurch können bereits bekannte Daten über die Person angegeben und somit die Suche verfeinert beziehungsweise verbessert werden.

Ziel 2 *Webseiten, die eine große Menge von personenbezogener Daten enthalten, auslesen und analysieren.*

Durch die zweite Suchfunktion soll eine große Menge an Daten gewonnen werden und dadurch ein weitläufiger Angriff zu simulieren Bei der zweiten Suchfunktion kann nur die Webseite angegeben werden, welche ausgelesen und analysiert werden soll. Durch diese Funktion ist es möglich einen weitläufigen Phishing-Mail-Angriff zu simulieren.

Ziel 3 *E-Mail-Adressen aus den gewonnen Daten generieren.*

Durch die Zusammensetzung von Vorname, Name und Geburtsjahr können E-Mail-Adressen generiert werden.

Ziel 4 *Anhand der oben genannten Klassifizierung werden Phishing-Mail-Muster erstellt*

Diese Muster können ebenfalls Klassifiziert werden. Das bedeutet, dass je nach gefunden Information ein passendes Muster vorhanden sein muss.

Ziel 5 *Phishing-Mail erzeugen.*

Mit der vorhandenen Information, der E-Mail-Adresse und einem passende Muster, wird eine Phishing erzeugt und versendet.

1.3 Eigene Leistung

In dieser Arbeit wird ein Tool erstellt, welches personenbezogene Daten automatisiert aus dem Internet heraussucht und diese in potentielle Opferprofile ablegt. Die gewonnenen Informationen werden automatisiert in eine personalisierte Phishing-E-Mail eingebaut. Für einen höheren Erfolg werden E-Mail-Muster erstellt.

Damit ein kompletter Ablauf eines Phishing-Mail-Angriffs simuliert werden kann, wird ein Algorithmus entwickelt, der aus den gewonnen Informationen eine E-Mail-Adresse generiert.

1.4 Aufbau der Arbeit

Die Arbeit gliedert sich in einem theoretischen und praktischen Teil auf. Der Theorie-Teil beginnt im zweiten Kapitel und beschreibt die Grundbegriffe im Bereich Social Engineering, Webtools, E-Mails und Programmiersprachen. Im nächsten Kapitel befindet sich die Anforderungsanalyse. Hier werden die Anforderungen an die Arbeit festgelegt. Darauf folgen die Lösungsvorschläge im Kapitel vier und die ausgewählte Lösung anhand den Anforderungen im Kapitel 5. Anschließend wird bei der Umsetzung auf den Praktischen Teil eingegangen.Am Ende befindet sich das Fazit, der Ausblick und der Anhang.

2 Grundlagen

2.1 Social Engineering

2.1.1 Definition

Die Definition von Social Engineering (SE) ist nicht eindeutig. Es gibt sehr verschiedene Ansichten von der Definition. Die Idee von Social Engineering ist, eine Ziel so zu manipulieren, damit das Ziel eine für den Angreifer bessere Entscheidung trifft. In dem Buch Social Engineering - The Art of Human Hacking, von Christopher Hadnagy, ist Social Engineering definiert als “social engineering is the act of manipulating a person to take an action that may or may not be in the “target’s“ best interest“ [Had11]. Die Definition in dem Buch von Kevin D. Mitnick lautet:“Social Engineering uses influence and persuasion to deceive people by convincing them that the social engineer is someone he is not, or by manipulation. As a result, the social engineer is able to take advantage of people to obtain information with or without the use of technology“ [Mit01].

2.1.2 SE im Alltag

SE wird einem von Geburt an beigebracht und begegnet einem beinahe jeden Tag. Schon ein Baby muss wissen wie es die Eltern manipulieren kann damit man Dinge wie Essen, Zuneigung, o.ä. bekommt. Darüber hinaus ist SE in vielen Berufen ein täglicher Bestandteil. Beispielsweise manipulieren Ärzte viele Patienten mit einer Placebo-Behandlung. Bei dieser Behandlung wird dem Patient ein wirkstoff-freies Medikament verschrieben. Nur durch die Manipulation des Patienten und den sogenannten Palzebo-Effekt können Erfolge erzielt werden.

2.1.3 SE in der Informationssicherheit

Im Bereich der Informationssicherheit spricht man von Social Engineering wenn man durch Manipulierung bzw. das Hacken von Menschen Passwörter, Zugänge zu Systemen oder vertrauliche Information bekommt. Die bekanntesten Angriffsmethoden sind Phishing, Pretexting, Baiting und Quad Pro Quo. Bei dieser Arbeit wird aber hauptsächlich auf das Thema Phishing eingegangen.

2.1.4 SE Angriffe

Aufbau eine SE-Angriffzykluses

Der Aufbau eines SE-Angriffes ist definiert in mehrere Phasen. Das wohl bekannteste Modell für einen Social Engineering-Angriffszyklus ist in dem Buch von Kevin D. Mitnicks - The art of deception: controlling the human element of security [Mit01] definiert. Dieser Zyklus besteht aus den 4 Phasen Research, Developing rapport and trust, Exploiting trust und Utilize information. In der Research-Phase geht es um die Informationsbeschaffung, bei der der Angreifer möglichst viel Informationen über das Ziel herausfindet. Die Developing rapport and trust Phase beschreibt den Aufbau für einen guten Kontakt, da der Angreifer ein leichteres Spiel hat wenn das Ziel dem Angreifer vertraut. Das nun erzeugte Vertrauen wird in der Exploitung trust Phase ausgenutzt. Hier will der Angreifer die eigentlich Information vom Opfer herausfinden. Dies geschieht einerseits durch bestimmtes nachfragen oder Manipulation. Utilize information ist die letzte Phase. Dort wird die gewonnene Information genutzt um das eigentliche Ziel des Angreifers zu erreichen.
Grundsätzlich werden bei einem Social Engineering Angriff menschliche Wünsche, Ängste und verbreitete Verhaltensmuster verwendet um ein Opfer zu manipulieren. [uDsiNe15]

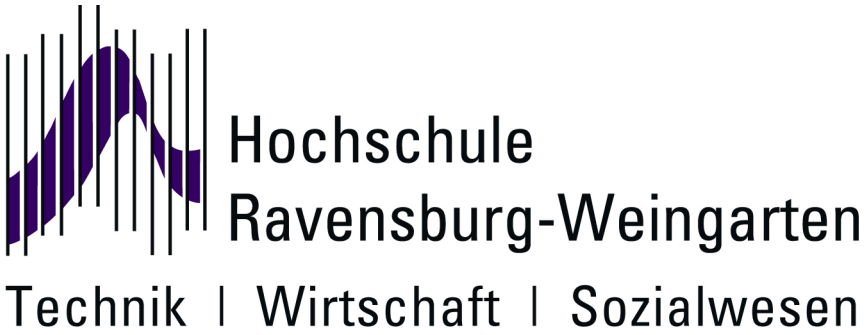


Bild 2.1: Logo der HS – oder nicht?

!!!!!!!!RICHTIGES BILD von ZYKLUS EINFÜGEN!!!!

SE Attack Framework

Leider sind die Phasen in dem Buch von Mintnick [Mit01] nicht sehr detailliert beschrieben. Aus diesem Grund haben die Autoren von der Publikation "Social Engineering Attack Framework" [FM14] ein Framework erstellt, was eine Erweiterung von Mitnick's Angriffszykluses darstellt.

!!!!!!!!RICHTIGES BILD von FRAMEWORK EINFÜGEN!!!!

Phishing

Das Wort Phishing wird von dem Wort "fishing" abgeleitet, da die Angreifer nach Informationen fischen. Das "Ph" kommt von "sophisticated" und meint damit, dass die Angreifer ausgeklügelte Techniken verwenden um an Informationen heranzukommen. [Jam05]
Phishing ist ein Angriffsmethode, bei dem ein Angreifer glaubwürdige E-Mails versendet, um von einem Opfer Informationen zu erhalten. Die sogenannten E-Mails enthalten meist eine Aufforderung einen Link zu öffnen und sehen täuschend echt aus. Zum Beispiel könnten der Angreifer ein Layout von Amazon verwenden und Sie auffordern, den Link zu öffnen, wegen einem Authentifizierungsproblem. Nachdem Sie auf den Link geklickt haben müssen Sie sich anmelden. Hier könnten die Angreifer Ihre Anmeldedaten abgreifen, nachdem Sie sie eingeben haben. Sobald Sie die Anmeldedaten haben könnten Sie mit der Meldung :"Hoppla,

ein Fehler ist aufgetreten, melden Sie sich bitte neu an!“ auf die originale Seite weitergeleitet werden. Durch diesen Vorgang hätten die Angreifer ihre Anmeldedaten bekommen.
Für diese Methode benötigt der Angreifer nicht nur Social Engineering Fähigkeiten sonder auch technische. [CH15]

Spear-Phishing

Spear-Phishing ist im Prinzip die gleiche Angriffsmethode wie Phishing. Der Unterschied besteht darin, dass anstatt einer anonymen E-Mail eine Mail an ein ausgewähltes Opfer gesendet wird. In einer Spear-Phishing-E-Mail wird ein Opfer beispielsweise mit einem Namen angesprochen oder es sind E-Mails mit Inhalten die das Opfer interessieren könnten. Aus diesem Grund benötigt man hier Zeit für die Informationsbeschaffung. Dennoch ist der Erfolg hier vielversprechender als beim normalen E-Mail-Phishing. Desweitern ist Spear-Phishing oft mit E-Mail-Spoofing verbunden. 91% der Advanced Persistent Threat (APT) Angriffe auf Firmen beginnen mit einer Spear-Phishing-E-Mail. Die Schadsoftware wir meisten als Remote Access Trojans (RATs) in einem Zip-Datei überliefert. [Cal13]

2.2 Webtools

2.2.1 Web Scraping

Definition

In der Theorie bedeutet web scraping die Informationsbeschaffung im Internet mit unterschiedlichsten Mitteln. [Mit15]

Funktionsweise

Meist wird dies mit einem automatisierten Programm realisiert, das Daten von einem Webserver anfragt, bekommt, analysiert und auswertet. In der Praxis gibt es ein großes Feld von Programmiertechniken und Einsatzmöglichkeiten. Mit Hilfe von web scraping ist es möglich große Datenmengen zu erfassen und verarbeiten. [Mit15]

2.2.2 Web Crawling

Definition

Beim Web Crawling werden Webinhalte geladen und nach Hyperlinks durchsucht. Diesen wird wieder gefolgt und der Prozess beginnt von vorne. Das ist die Grundfunktion einer Suchmaschine. ???? Crawler. [Mit15]

Funktionsweise

Die Funktionsweise besteht darin, dass in den meisten Fällen ein automatisiertes Programm, Web Crawler, erstellt wird. Der Web Crawler lädt Webinhalte runter und durchsucht diese nach Hyperlinks bzw. URLs. Den gefundenen Hyperlinks werden wieder gefolgt, um neue Webseiten mit weiteren URLs zu laden. So hangelt sich ein Web Crawler von Link zu Link durch das Internet. [Mit15]

2.3 Personenbezogene Daten

2.3.1 Definition

Laut DSGVO sind personenbezogene Daten “alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;“ [DSG]

3 Problemspezifikation

Persönliche Daten sind im Internet oft frei zugänglich. Das heißt, dass unterschiedlichste Webseiten persönliche Information von Menschen öffentlich bereitstellen. Die bekanntesten Webseiten sind wahrscheinlich die Social Media Seiten wie Twitter, Facebook und Instagram. Allerdings wird auch auf anderen Webseiten personenbezogene Daten in großen Mengen bereitgestellt. Ein Beispiel dafür ist das Fußballportal “www.fupa.net“. Diese Art von Webseiten sind perfekte Informationsquelle für Phisher.
Im Bereich von Social Engineering Angriffen wird diese Information oft genutzt um ein Opfer zu täuschen oder manipulieren.
Dass hier beschriebene Problem zeigt, dass der Zugang für persönliche Information durch das Internet für die Öffentlichkeit einfacher gemacht wird. Es soll mit einem kritisch Blick darauf gezeigt werden, wie einfach es ist, personenbezogene Daten aus dem Internet herauszulesen, analysieren und für einen Phishing-Angriffe zu verwenden.

4 Anforderungsanalyse und Priorisierung

4.1 Anforderungsanalyse

Die im Kapitel 1.2 definierten Ziele sollen mit den folgenden Anforderungen gewährleistet werden.

4.1.1 Anforderung an die Informationsbeschaffung

Die Anforderungen an die Informationsbeschaffung von personenbezogenen Daten lässt sich in zwei Teile gliedern. Erstens in die Informationsbeschaffung von bestimmten bzw. ausgewählten Personen und zweitens die Informationsbeschaffung von einer großen Menge unbestimmter Personen.

Informationsbeschaffung von bestimmten/ausgewählten Personen

Bei dieser Informationsbeschaffung soll eine Suchfunktion entwickelt werden, welche Informationen zu einer angegeben Person sucht. Dies soll mit Hilfe eines Web-Crawlers und mit einem Web-Scraper umgesetzt werden. Das zu entwickelnde Tool soll bekannte Information/Daten (Name, Geburtsjahr, Ort, Usernames von Social Media Webseiten) über eine Konsolen-Abfrage einlesen können. Die Herausforderung besteht darin, zu erkennen, wann und ob es sich um die Information der gesuchten Person handelt.

Informationsbeschaffung von unbestimmten Personen

Es soll eine Prototyp-Suchfunktion entwickelt werden, die eine komplette Website durchsucht und möglichst viele Informationen von möglichst vielen Personen herausfindet. Jedoch sind diese Personen dem Tool-Anwender unbekannt. Die Informationen werden aus Webseiten mit

einer großen Anzahl von Mitgliedern herausgelesen. Bei dem Prototyp soll es möglich sein, aus vorgegebenen Webseiten ein auszuwählen, die anschließend ausgelesen werden soll.

4.1.2 Anforderung an die Datenverwaltung/-speicherung

Ausgelesene Daten sollen vor dem speichern formatiert und klassifiziert werden, damit die Daten später korrekt in die Phishing-Mails eingesetzt werden können. Die Schwierigkeit besteht darin, zu erkenn wann es sich beispielsweise um ein Hobby oder Beruf zu erkennen. Webseiten müssen analysiert und ausgewertet werden. Zusätzlich sollen die Daten in einer gut übersichtlichen Struktur gespeichert werden und müssen beliebig erweiterbar sein.

4.1.3 Anforderung an die Generierung der E-Mail-Adressen

Da nicht zu jeder Suche eine E-Mail-Adresse im Internet gefunden werden kann, muss die E-Mail-Adresse aus den vorhandenen Informationen generiert werden. Es soll eine größere Anzahl von möglichen E-Mail-Adressen generiert werden, damit die Wahrscheinlichkeit größer wird, dass die richtige E-Mail-Adresse dabei ist. Zusätzlich kann geprüft werden, ob die E-Mail-Adresse verwendet wird.

4.1.4 Anforderung an die E-Mail-Muster

E-Mail-Muster sollen erstellt werden und so klassifiziert sein, dass für jedes gefundene Opferprofil ein passendes Muster vorhanden ist. Des Weiteren soll der E-Mail-Text so gewählt sein, damit er Sinn ergibt und eine korrekte Grammatik beinhaltet.

4.1.5 Anforderung an die Erstellung der Phishing-Mail

Die Phishing-Mails sollen automatisiert erstellt werden. Die Auswahl des richtigen E-Mail-Musters zu der gewonnenen Opferinformation soll ebenfalls automatisiert ablaufen.

4.1.6 Unter anderem soll die Arbeit Antworten auf folgende Fragen finden:

??

Tabelle 4.1: Priorisierung der Anforderungen

Anforderung	Priorisierung (A-C)
Informationsbeschaffung von ausgewählten Personen	*A*
Informationsbeschaffung von vielen ubekannten Personen	*A*
E-Mail-Muster erstellen	*A*
Phsishing-Mail erzeugen	*B*
Datenverwaltung/-speicherung	*B*

4.2 Priorisierung

Die Tabelle 4.1 zeigt die Priorisierung der Anforderungen.

Man beachte: Bilder haben Bild**unter**schriften, Tabellen haben Tabellen**über**schriften.

5 Lösungsideen

Für die Umsetzung der im Kapitel 1.2 definierten Ziele, werden folgende Lösungsideen vorgeschlagen.

5.1 Informationsbeschaffung

Für die Eingabe von Suchdaten, besteht für beide Informationsbeschaffungen die Möglichkeit eine Grafische-Bedienoberfläche oder eine Konsolen-Eingabe zu verwenden.

5.1.1 Informationsbeschaffung von bestimmten/ausgewählten Personen

Verschiedenste Webseiten durchsuchen. Ideen dafür sind Facebook, FuPa, Instagram, Xing, LinkedIn, Google und Twitter. Damit geschaut werden kann ob es sich um die gleiche Person auf unterschiedlichen Webseiten handelt, können folgenden Ideen angewendet werden:
- je nach vorgegeben Daten kann erst auf den entsprechenden Webseiten gesucht werden (Username von Instagram –> dann erste Seite Instagram, Voller Name und Ort –> Xing, LinkedIn, Google, Geburtsjahr und Name –> FuPa)
- bei keiner perfekten Übereinstimmung wird Suche erweitert. D.h. es wird zusätzlich in Verbindung mit Facebook-Freunden, FuPa-Teammitglieder, oder Xing-Arbeitskollegen gesucht)
-Profilbilder können verglichen werden. Entweder mit Bilderkennungssoftware oder Googl-Bildersuche)
-Google Suche verfeinern mit Hilfe von Open Source Intellicence Techniques

5.1.2 Informationsbeschaffung von einer großen Menge unbestimmter Personen

Webseiten mit großen Menge von Daten, ausgenommen von den bekannten Social Media Seiten, sind das Fußballportal FuPa, Xing und LinkedIn.

5.2 Datenanalyse/-speicherung

Für die Datenanalyse kann ein Text-Analyse-Tool verwendet werden, damit die Texte von einer Webseite, vor dem Speichern, korrekt interpretiert und nach Schlüsselwörter untersucht werden können. Des Weiteren kann ein Algorithmus entwickelt werden, der nach Schlüsselwörtern in einer Webseite sucht.Bei der Datenspeicherung wird erneut nach der Art der Informationsbeschaffung unterschieden. Für die Suche einzelner Person, kann ein erweiterbares Personen-Objekt erstellt werden. Für die Informationsbeschaffung von vielen unbekannten Personen, könnte eine SQL-Datenbank erstellt werden. Ein weiterer Vorschlag wäre, eine Datei anzulegen, bei der alle Personen gut strukturiert gespeichert werden können. Möglichkeiten dafür wären die Dateiformate CSV und TXT.

5.3 Generierung der E-Mail-Adressen

Kann das opensource tool von inteltechniques mit Hilfe eines automatisierten Webbrowsers verwendet werden. Algorithmus entwickeln, der alle möglichen Mail-Adressen aus den Daten Vorname, Nachname, Geburtsjahr und den bekanntesten Mail-Providern erzeugt.

5.4 Erstellung der E-Mail-Muster

Die Muster können in zwei große Kategorien unterteilt werden. Es gibt einen privaten und geschäftlichen Teil. Der private Teil hat weiter Unterteilungen wie Familie, Hobby/Interessen.

5.5 Erzeugung der Phishing-Mail

6 Auswahl der Lösung anhand den Anforderungen

6.1 Informationsbeschaffung

6.1.1 Informationsbeschaffung von bestimmten/ausgewählten Personen

6.1.2 Informationsbeschaffung von einer großen Menge unbestimmter Personen

6.2 Datenanalyse/-speicherung

6.3 Generierung der E-Mail-Adressen

6.4 Erstellung der E-Mail-Muster

6.5 Erzeugung der Phishing-Mail

7 Umsetzung

7.1 Informationsbeschaffung von der Website www.fupa.net

7.1.1 Erstellung eines Web Crawlers

Anforderung

Der Web Crawler soll die komplette Webseite www.fupa.net durchgehen und Links mit Spielerinformationen speichern. Die Funktionsweise des Web Crawlers besteht darin, dass das Programm auf der Startseite von Fupa.net beginnt nach links zu suchen und diesen folgt.

Probleme

1. Python hat einen verkürzten und erkennbaren Standard http-Header. Dieser wird von vielen Administratoren geblockt und mit der Fehlermeldung 451 erkennbar gemacht. 451 for legal reason
2. Honeypots gewollt oder ungewollt, hier Kalender darstellung mit links zu neuen Jahren die eine sehr hohe bis überhaupt keine Begrenzung haben.
3. Rekursion erreicht schnell die Maximale tiefe von 1500.
4. Zu langsamer Algorithmus

Lösungen

1. http-Header selber konfigurieren
2. Links mit möglichen Honeypots nicht beachten
3. Stack Klasse schreiben damit keine Rekursion benötigt wird
4. Algorithmus anpassen auf fupa-Webseite

7.2 Datenverwaltung und Speicherung

7.2.1 Speicherung von Personendaten in CSV oder mySQL

8 Hauptteil

8.1 Hauptteil

8.1.1

9 Hauptteil

9.1 Hauptteil

9.1.1

10 Hauptteil

10.1 Hauptteil

10.1.1

11 Hauptteil

11.1 Hauptteil

11.1.1

12 Schlussbemerkungen und Ausblick

A Ein Kapitel des Anhangs

Glossar

Active Directory

Active Directory ist in einem Windows Server 2000, Windows Server 2003, oder Windows Server 2008-Netzwerk der Verzeichnisdienst, der die zentrale Organisation und Verwaltung aller Netzwerkressourcen erlaubt. Es ermöglicht den Benutzern über eine einzige zentrale Anmeldung den Zugriff auf alle Ressourcen und den Administratoren die zentral organisierte Verwaltung, transparent von der Netzwerktopologie und den eingesetzten Netzwerkprotokollen. Das dafür benötigte Betriebssystem ist entweder Windows Server 2000, Windows Server 2003, oder Windows Server 2008, welches auf dem zentralen Domänencontroller installiert wird. Dieser hält alle Daten des Active Directory vor, wie z.B. Benutzernamen und Kennwörter. 3

Glossareintrag

Erweiterte Informationen zum einem Wort oder einer Abkürzung, ähnlich einem Eintrag im Duden. 3

AbkÃ¼rzungsverzeichnis

AD Active Directory 3

Symbolverzeichnis

π	Die Kreiszahl. 3

Literatur

[All18] Allensbach, IfD: *Meistgenutzte Informationsquellen der Bevlkerung in Deutschland im Jahr 2018.* https://de.statista.com/statistik/daten/studie/171257/umfrage/normalerweise-genutzte-quelle-fuer-informationen/, 2018. Abrufdatum: 18.01.2019.

[Bun18] Bundeskriminalamt: *Polizeilich erfasste Fälle von Cyberkriminalität im engeren Sinne* in Deutschland von 2004 bis 2017.* https://de.statista.com/statistik/daten/studie/295265/umfrage/polizeilich-erfasste-faelle-von-cyberkriminalität-im-engeren-sinne-in-deu 2018. Abrufdatum: 29.10.2018.

[Cal13] Caldwell, Tracey: *Spear-phishing: how to spot and mitigate the menace.* Computer Fraud & Security, 2013(1):11–16, 2013.

[CH15] Christopher Hadnagy, Michele Fincher: *Phishing Dark Waters: The Offensive and Defensive Sides of Malicious E-mails.* 2015.

[DSG] DSGVO: *Art. 4 DSGVO Begriffsbestimmungen.* https://dsgvo-gesetz.de/art-4-dsgvo/. Abrufdatum: 09.01.2019.

[FM14] Francois Mouton, Mercia M. Malan, Louise Leenen H.S. Venter: *Social Engineering Attack Framework.* 2014.

[Had11] Hadnagy, Christopher: *Social Engineering: The Art of Human Hacking.* 2011.

[Jam05] James, Lance: *Phshing Exposed: Uncover Secrets from the Dark Side.* 2005.

[Mit01] Mitnick, Kevin D.: *The art of deception:controlling the human elemnet of security.* 2001.

[Mit15] Mitchell, Ryan: *Web Scraping with Python: Collecting Data from the Modern Web.* 2015.

[NW18] Nordrhein-Westfalen, Verbraucherzentrale: *Phishing-Radar: Aktuelle Warnungen.* https://www.verbraucherzentrale.nrw/wissen/digitale-welt/phishingradar/phishingradar-aktuelle-warnungen-6059, 2018. Abrufdatum: 29.10.2018.

[uDsiNe15] Netz e.V., DATEV und Deutschland sicher im: *Verhaltensregeln zum Thema "Social Engineering"*. 2015.