



GuT Workshop Agenda



- IT Sicherheit als TOP Thema im Wahljahr
- IT Sicherheit im Unterricht am Berufskolleg
- Netacad Cybersecurity „Introduction“ oder „Essentials“
- Einstiegshürden
- Beispiele für Lernmaterial im Kurs
- Didaktische Überlegungen und Lernsituationen
- Diskussion

GuT Wichtige Fragen...

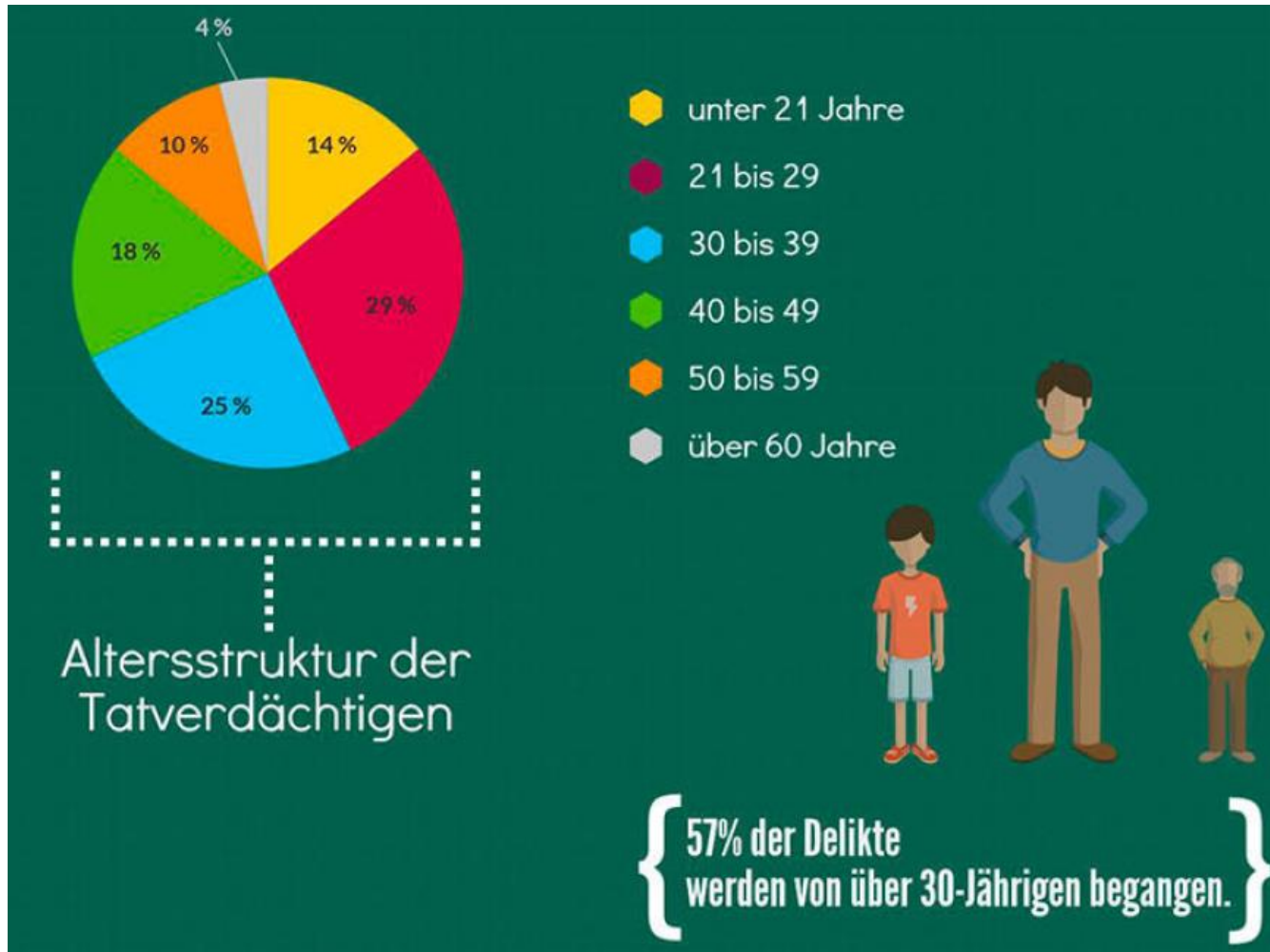


- Sind Sie über 30 Jahre alt?
- Sind sie männlich?
- Sind Sie verdächtig?

JA !



Quelle: Bundeskriminalamt – Infografik Cybercrime



Polizeiliche Kriminalstatistik Nordrhein-Westfalen

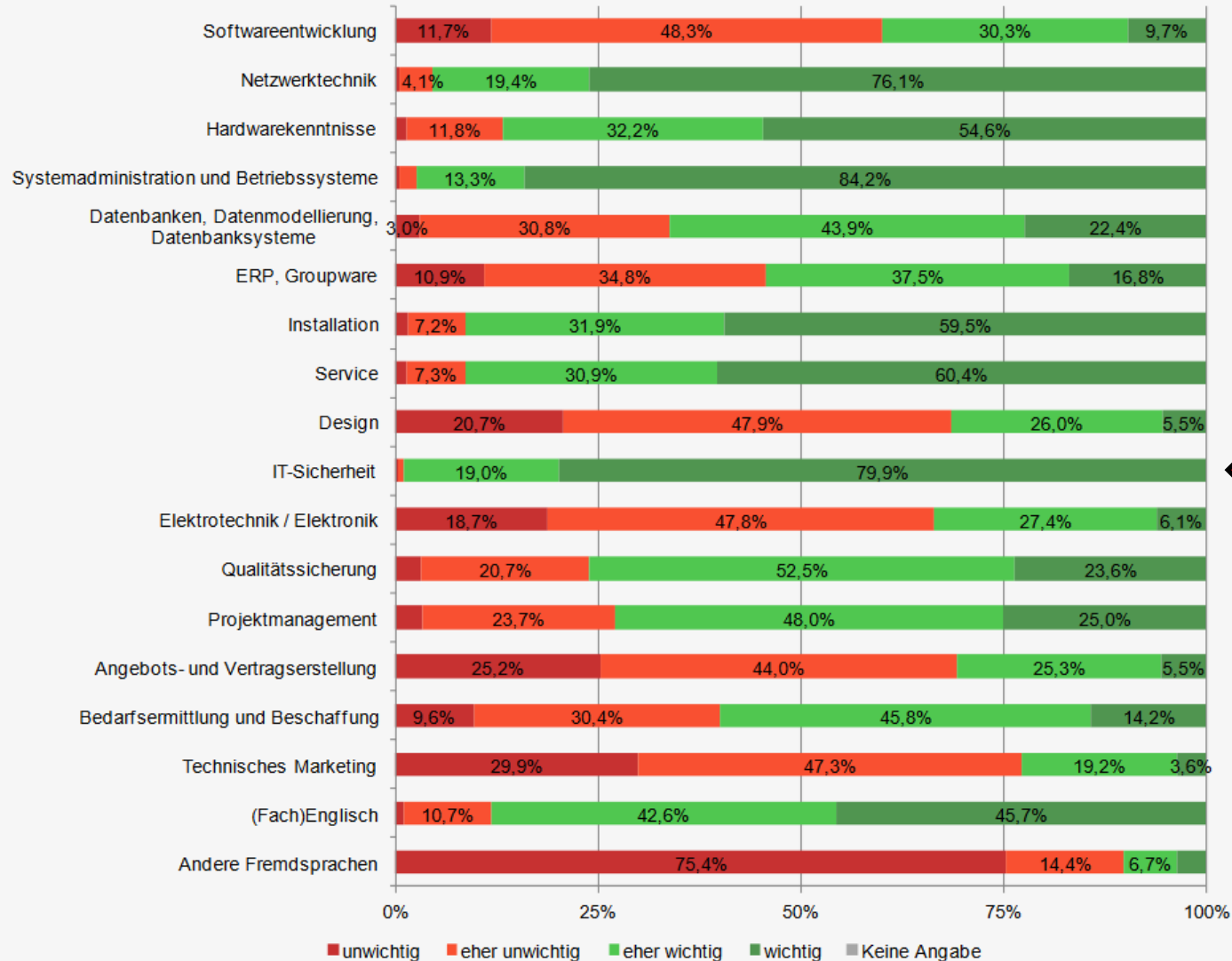
Tatmittel Internet Entwicklung der Fallzahlen

Schl.-	Straftat	2015			2016			
		Bekanntg.	Aufgekl.	AQ	Bekanntg.	Aufgekl.	AQ	
		Fälle	Fälle	%	Fälle	Fälle	%	
897000	Computerkriminalität	9 012	2 185	24,25	12 903	3 586	27,79	+3 891
897100	Computerbetrug § 263a StGB				7 645	2 729	35,70	+7 645

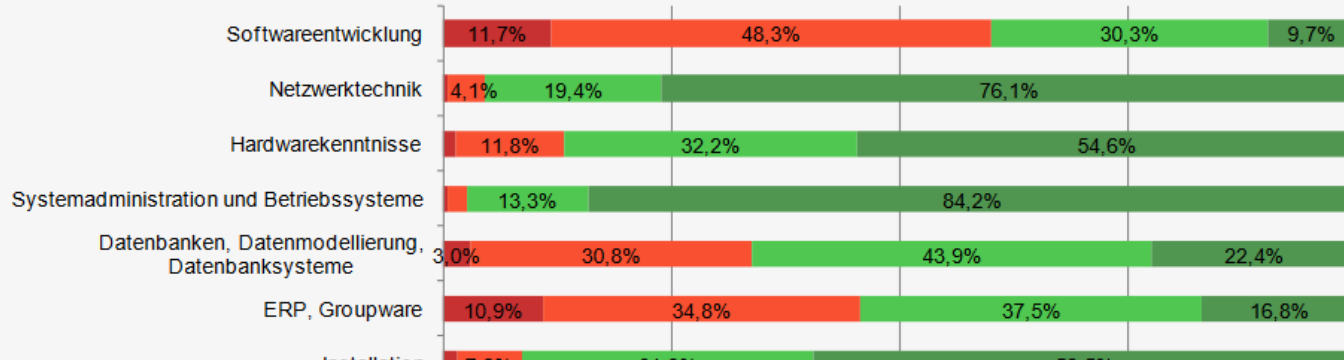
Steigerung um 44%
2015 → 2016

- In den Lehrplänen kaum zu finden
 - In wenigen/Worten oder Stichworten
 - Alter der Pläne > 10 Jahre
 - KMK Rahmenlehrplan FISl(1998)
 - Landeslehrplan FISl (2005)
- Interesse ist aber auf allen Seiten groß!

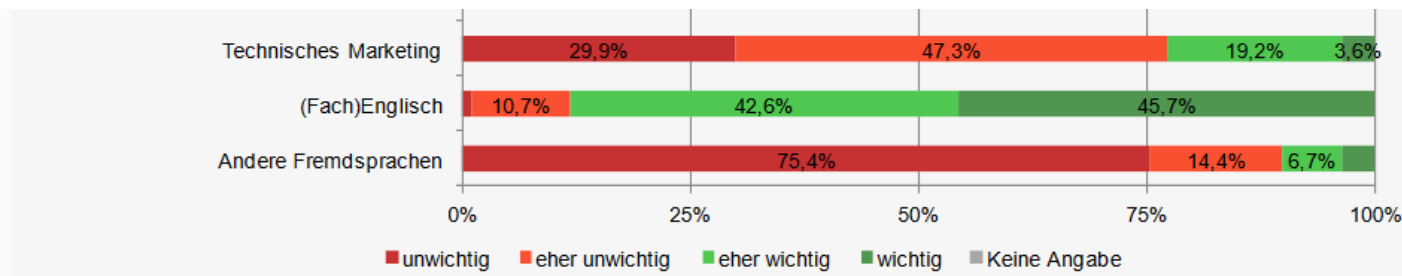
Fachinformatiker/in – Systemintegration: IT-Fachkräfte (N=513), Ausbildungsverantwortliche (N=645), Personalverantwortliche (N=312), Lehrkräfte (N=134), Gesamt (N=1603)



Fachinformatiker/in – Systemintegration: IT-Fachkräfte (N=513), Ausbildungsverantwortliche (N=645), Personalverantwortliche (N=312), Lehrkräfte (N=134), Gesamt (N=1603)



IT-Sicherheit





Certificate of Completion

Presented to:

Max Mustermann

Name

For completing the Cisco Networking Academy® Introduction to Cybersecurity course, and demonstrating the ability to explain the following:

- Global implications of cyber threats
- Ways in which networks are vulnerable to attack
- Impact of cyber-attacks on industries
- Cisco's approach to threat detection and defense
- Why cybersecurity is a growing profession
- Opportunities available for pursuing network security certifications

Musterinstruktor

Instructor



Instructor Signature

Mar 13 2017

Date

BEISPIEL

BEISPIEL

BEISPIEL

BEISPIEL

BEISPIEL

BEISPIEL

BEISPIEL

GuT Workshop Agenda



- IT Sicherheit als TOP Thema im Wahljahr
- IT Sicherheit im Unterricht am Berufskolleg

Netacad Cybersecurity „Introduction“ oder „Essentials“

- Einstiegshürden
- Beispiele für Lernmaterial im Kurs
- Didaktische Überlegungen und Lernsituationen
- Diskussion

Einführung in die Cybersicherheit

Kapitel 0

Kurseinleitung

Kapitel 1

Die Notwendigkeit von Cybersicherheit

Kapitel 2

Angriffe, Konzepte und Techniken

Kapitel 3

Schützen Ihrer Daten und Privatsphäre

Kapitel 4

Schützen des Unternehmens

Kapitel 5

Liegt Ihre Zukunft in der Cybersicherheit?

GuT Ansatz – Langer Kurs



Cybersecurity Essentials – Grundlagen der Cybersicherheit

Kapitel 0

Kurseinführung

Kapitel 1

Cybersicherheit – eine Welt von Hexenmeistern, Helden und Kriminellen

Kapitel 2

Der Hexenmeister-Würfel der Cybersicherheit

Kapitel 3

Cybersicherheitsbedrohungen, Sicherheitslücken und Angriffe

Kapitel 4

Die Kunst, Geheimnisse zu schützen

Kapitel 5

Die Kunst, Integrität zu gewährleisten

Kapitel 6

99,999 % – Hochverfügbarkeit

Kapitel 7

Stärkung der Abwehr

Kapitel 8

Spezialist für Cybersicherheit werden



GuT Verglichen

Kapitel 0

Kurseinleitung

Kapitel 1

Die Notwendigkeit von Cybersicherheit

Kapitel 2

Angriffe, Konzepte und Techniken

Kapitel 3

Schützen Ihrer Daten und Privatsphäre

Kapitel 4

Schützen des Unternehmens

Kapitel 5

Liegt Ihre Zukunft in der Cybersicherheit?

Kapitel 0

Kurseinführung

Kapitel 1

Cybersicherheit – eine Welt von Hexenmeistern, Helden und Kriminellen

Kapitel 2

Der Hexenmeister-Würfel der Cybersicherheit

Kapitel 3

Cybersicherheitsbedrohungen, Sicherheitslücken und Angriffe

Kapitel 4

Die Kunst, Geheimnisse zu schützen

Kapitel 5

Die Kunst, Integrität zu gewährleisten

Kapitel 6

99,999 % – Hochverfügbarkeit

Kapitel 7

Stärkung der Abwehr

Kapitel 8

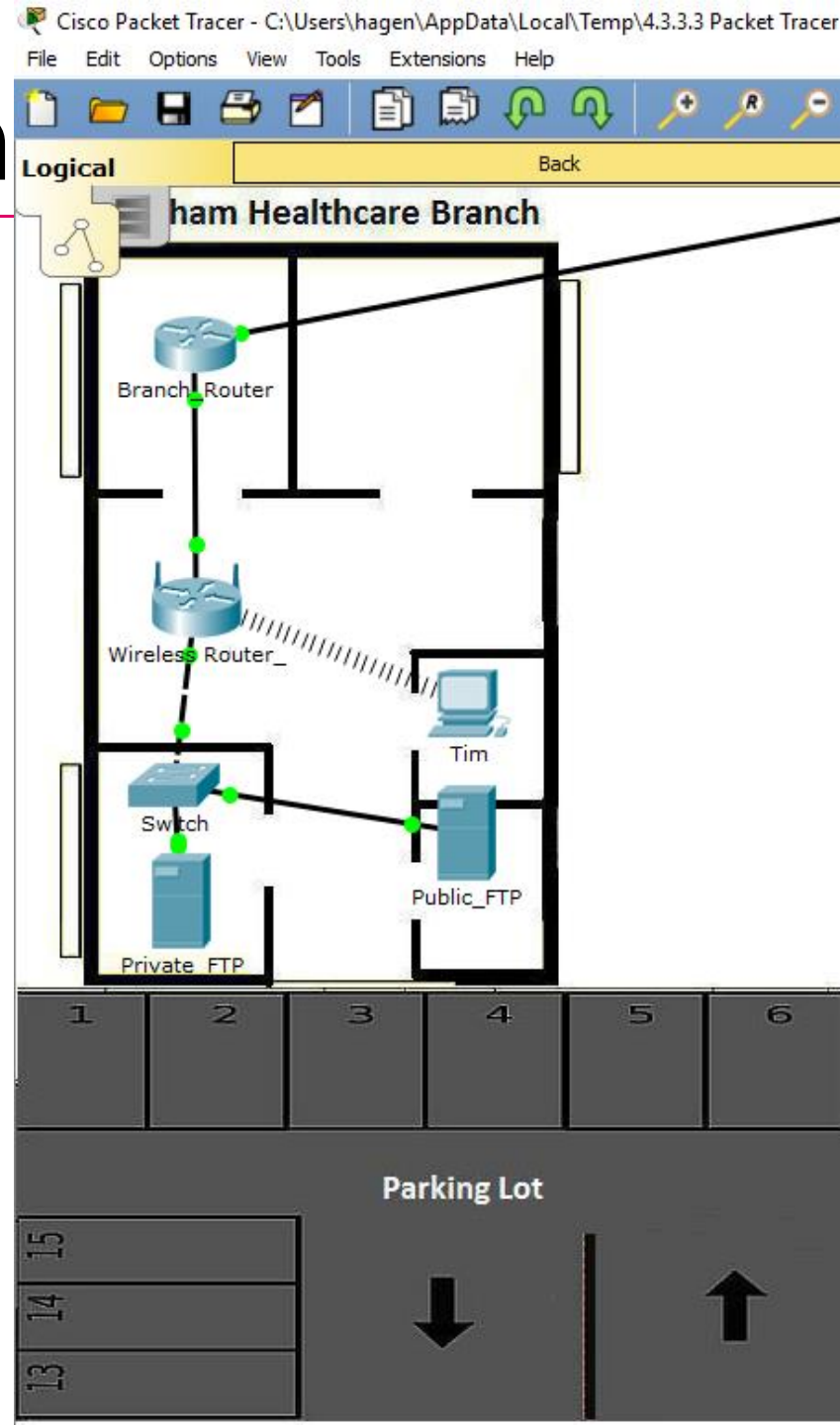
Spezialist für Cybersicherheit werden

GuT VPN im Cybersecurity Essentials



GuT PT-Übungen

- Schüler können VPNs konfigurieren
- Praxisnahe Simulation
- Überschaubare Situationen



GuT Workshop Agenda



- IT Sicherheit als TOP Thema im Wahljahr
- IT Sicherheit im Unterricht am Berufskolleg
- Netacad Cybersecurity „Introduction“ oder „Essentials“
- ➔ Einstiegshürden
 - Beispiele für Lernmaterial im Kurs
 - Didaktische Überlegungen und Lernsituationen
 - Diskussion



My NetAcad | News and Events | Support | Res...

Berufskolleg fuer Gestaltung und Technik Aachen - CA

Course Name: ETVZ61SECUR_DE | Course ID: ETVZ61SECUR_DE
Start Date: 01/24/2017 | End Date: 05/31/2017



Administration der Kursdaten

NetAcad Offering: Introduction to Cybersecurity - German - 2.0
Language and Version: German 2.0

Instructor(s)
Instructors



Sinnvollerweise: 2 Instruktoren

<input type="checkbox"/>	First Name	Last Name	Email
<input type="checkbox"/>	Klaus	Hegemann	
<input type="checkbox"/>	Hagen	Hussmann	hagen.hussmann@berufskolleg-aachen.de

Keine Schulung erforderlich!

Get All Certificates

Get All Letters

Student(s)

Enrolled Students: 21



Viele, viele hochmotivierte Student(s)

20 Items per Page | Page 1 of 2 | Showing 1 - 20 of 21 results.

← First | Previous | Next | Last →

<input type="checkbox"/>	First Name	Last Name	Screen Name	Email	Last Login	Reset Password	Certificates/Letters
--------------------------	------------	-----------	-------------	-------	------------	----------------	----------------------

- Informative Texte und ansprechende Abbildungen
- Lab-Übungen – Anleitungen liegen als PDF-Dateien vor
- Recherche-Übungen
- Videos



Ansprechendes
Design der
Abbildungen



Ihre Online- und Offline-Identität

Je mehr Zeit Sie online verbringen, desto wichtiger ist Ihre Online- und Offline-Identität für Ihr Leben. Ihre Offline-Identität ist die Person, mit der Ihre Freunde und Familie täglich zuhause, in der Schule oder bei der Arbeit interagieren. Diese Personen kennen ihre persönlichen Informationen wie Ihren Namen, Ihr Alter und Ihren Wohnort. Ihre Online-Identität ist Ihr Auftreten im Cyberspace. Ihre Online-Identität wird dadurch bestimmt, wie Sie sich anderen Personen gegenüber online darstellen. Diese Online-Identität sollte nur eingeschränkte Informationen über Ihre Person enthüllen.


Überlegen Sie sich gut, welche Benutzer- oder Aliasnamen Sie für Ihre Online-Identität verwenden. Der Benutzername sollte keine persönlichen Informationen enthalten. Wählen Sie einen angemessenen und respektvollen Namen. Ihr Benutzername sollte Fremde nicht dazu verleiten, Sie als ...

Das (dunkle) Layout kann verändert werden!




Kapitel 1 Die Notwendigkeit von Cybersicherheit
▶ 1.3 Angreifer und Cybersicherheitsexperten
▶ 1.3.1 Profil eines Cyberangreifers
▶ 1.3.1.1 Angreifertypen
✕


White, Black und Grey Hat-Hacker



White Hat-Hacker



Grey Hat-Hacker



Black Hat-Hacker

White Hat-Hacker

Dies sind ethische Hacker, die ihre Programmierungsfähigkeiten für gute, ethische und legale Zwecke nutzen. White Hat-Hacker führen Eindringversuche in Netzwerke und Systeme durch, indem sie ihr Wissen über Computersicherheitssysteme verwenden, um Netzwerkrisiken zu erkennen. Sicherheitslücken werden den Entwicklern gemeldet, damit diese Schwachstellen geschlossen werden, bevor sie zu einer Bedrohung werden können. Einige Organisationen vergeben Preise oder Prämien an White Hat-Hacker, wenn sie sie über eine Schwachstelle informieren.

Angreifertypen

Angreifer sind Einzelpersonen oder Gruppen, die Sicherheitslücken ausnutzen, um sich persönliche oder finanzielle Vorteile zu verschaffen. Die Angreifer interessieren sich für Kreditkarten, Produktdesigns und alle sonstigen Dinge, die wertvoll sein könnten.


Amateure - Diese Personen werden manchmal auch Script Kiddies genannt. Diese Angreifer haben oft kaum oder keine Kenntnisse und verwenden im Internet verfügbare Tools für ihre Angriffe. Manche von ihnen sind einfach nur neugierig, und andere möchten ihr Können unter Beweis stellen und Schäden anrichten. Obwohl sie einfache Tools verwenden, können die Folgen dennoch verheerend sein.

Hacker - Diese Gruppe von Angreifern bricht in Computer oder Netzwerke ein, um sich Zugriff zu verschaffen. Je nach Motiv für den Einbruch werden diese Angreifer nach White Hat, Grey Hat und Black Hat unterschieden. White Hat-Hacker brechen in Netzwerke oder Computersysteme ein, um Schwachstellen zu finden, damit die Sicherheit dieser Systeme verbessert werden kann. Diese Einbrüche erfolgen mit vorheriger Genehmigung, und die Ergebnisse werden dem Eigentümer gemeldet. Black Hat-Hacker machen sich

🗨️ 🔖 ⏪ ⏩

Kapitel 1
Die Notwendigkeit von Cybersicherheit
▶ 1.3
Angreifer und Cybersicherheitsexperten
▶ 1.3.1
Profil eines Cyberangreifers
▶ 1.3.1.1
Angriffertypen
X

White, Black und Grey Hat-Hacker




Grey Hat-Hacker X

Dies sind Personen, die Verbrechen begehen und unmoralische Aktionen durchführen, aber nicht um sich persönlich zu bereichern oder Schaden anzurichten. Beispiel könnte jemand sein, der ein Netzwerk ohne Erlaubnis kompromittiert und dann die Schwachstellen öffentlich meldet. Ein Grey Hat-Hacker gibt möglicherweise eine Schwachstelle der betroffenen Organisation über ihr Netzwerk bekannt nachdem er es kompromittiert hat. Dies ermöglicht der Organisation das Problem zu beheben.

White Hat-Hacker

Grey Hat-Hacker

Black Hat-Hacker



Angriffertypen

Angreifer sind Einzelpersonen oder Gruppen, die Sicherheitslücken ausnutzen, um sich persönliche oder finanzielle Vorteile zu verschaffen. Die Angreifer interessieren sich für Kreditkarten, Produktdesigns und alle sonstigen Dinge, die wertvoll sein könnten.


Amateure – Diese Personen werden manchmal auch Script Kiddies genannt. Diese Angreifer haben oft kaum oder keine Kenntnisse und verwenden im Internet verfügbare Tools für ihre Angriffe. Manche von ihnen sind einfach nur neugierig, und andere möchten ihr Können unter Beweis stellen und Schäden anrichten. Obwohl sie einfache Tools verwenden, können die Folgen dennoch verheerend sein.

Hacker – Diese Gruppe von Angreifern bricht in Computer oder Netzwerke ein, um sich Zugriff zu verschaffen. Je nach Motiv für den Einbruch werden diese Angreifer nach White Hat, Grey Hat und Black Hat unterschieden. White Hat-Hacker brechen in Netzwerke oder Computersysteme ein, um Schwachstellen zu finden, damit die Sicherheit dieser Systeme verbessert werden kann. Diese Einbrüche erfolgen mit vorheriger Genehmigung, und die Ergebnisse werden dem Eigentümer gemeldet. Black Hat-Hacker machen sich

🗨
📖
⏪
⏩

Kapitel 1
Die Notwendigkeit von Cybersicherheit
▶ 1.3
Angreifer und Cybersicherheitsexperten
▶ 1.3.1
Profil eines Cyberangreifers
▶ 1.3.1.1
Angreifertypen
✕


White, Black und Grey Hat-Hacker



White Hat-Hacker



Grey Hat-Hacker



Black Hat-Hacker

Black Hat-Hacker

Dies sind unmoralische Kriminelle, die Computer und die Netzwerksicherheit aufgrund persönlicher Motive verletzen, oder auch in böser Absicht Netzwerke angreifen. Black Hat-Hacker nutzen Sicherheitslücken aus, um Computer und Netzwerksysteme zu kompromittieren.

Angreifertypen

Angreifer sind Einzelpersonen oder Gruppen, die Sicherheitslücken ausnutzen, um sich persönliche oder finanzielle Vorteile zu verschaffen. Die Angreifer interessieren sich für Kreditkarten, Produktdesigns und alle sonstigen Dinge, die wertvoll sein könnten.

Amateure – Diese Personen werden manchmal auch Script Kiddies genannt. Diese Angreifer haben oft kaum oder keine Kenntnisse und verwenden im Internet verfügbare Tools für ihre Angriffe. Manche von ihnen sind einfach nur neugierig, und andere möchten ihr Können unter Beweis stellen und Schäden anrichten. Obwohl sie einfache Tools verwenden, können die Folgen dennoch verheerend sein.

Hacker – Diese Gruppe von Angreifern bricht in Computer oder Netzwerke ein, um sich Zugriff zu verschaffen. Je nach Motiv für den Einbruch werden diese Angreifer nach White Hat, Grey Hat und Black Hat unterschieden. White Hat-Hacker brechen in Netzwerke oder Computersysteme ein, um Schwachstellen zu finden, damit die Sicherheit dieser Systeme verbessert werden kann. Diese Einbrüche erfolgen mit vorheriger Genehmigung, und die Ergebnisse werden dem Eigentümer gemeldet. Black Hat-Hacker machen sich

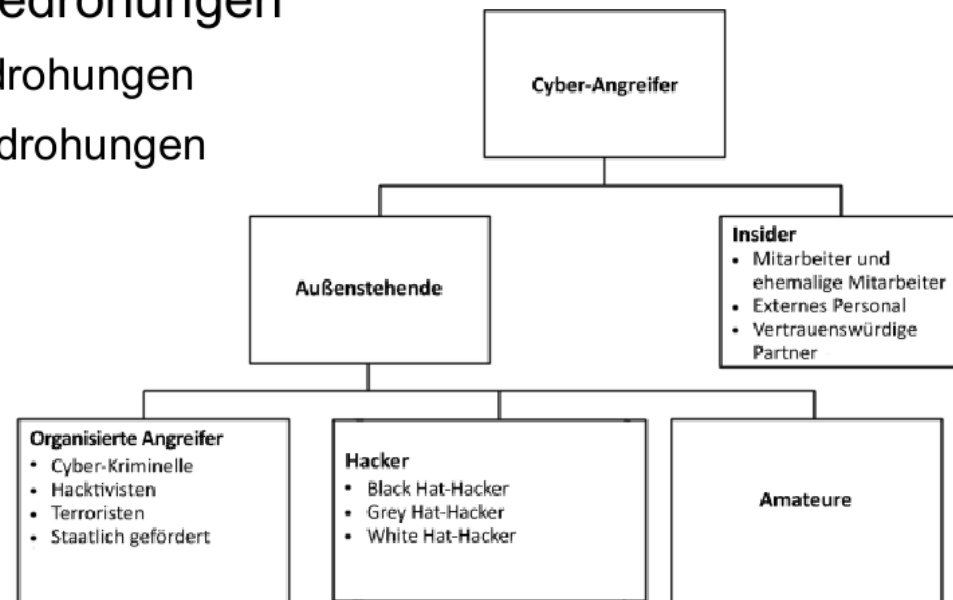
✕
🗨
📖
⏪
⏩



Angreifer und Cybersicherheitsexperten

Profil eines Cyberangreifers

- Angreifertypen
 - White Hat-Hacker
 - Grey Hat-Hacker
 - Black Hat-Hacker
- Interne und externe Bedrohungen
 - Beispiele für interne Bedrohungen
 - Beispiele für externe Bedrohungen





Analyse eines Cyberangriffs

Malwaretypen und Symptome

■ Arten von Malware

- Spyware
- Bot
- Ransomware
- Scareware
- Rootkit
- Man-in-The-Middle-Angriffe
- Können Sie einige weitere nennen?

■ Symptome von Malware

- Gelöschte Dateien
- Geänderte Dateien
- Können Sie weitere Symptome nennen?

Instruktorenfolien
sehr „knapp“ ☹️



Übung – Verwenden von Steganografie

Zielsetzung

Verstecken Sie mithilfe von Steganografie ein Dokument in einer JPEG-Datei.

Hintergrund/Szenario

Steghide ist ein Open-Source-Programm für Steganografie, das zum Verstecken von Daten in verschiedenen Dateitypen (z. B. Audio- und Bilddateien) verwendet wird. Bei dieser Übung verstecken Sie eine Datendatei in einer Bilddatei.

Erforderliche Ressourcen

- PC mit Ubuntu 16.04 Desktop LTS, auf einem virtuellen VirtualBox- oder VMware-System installiert

Schritt 1: Öffnen Sie in Ubuntu ein Terminalfenster.

- a. Melden Sie sich mit den folgenden Anmeldeinformationen in Ubuntu an:

Benutzer: **cisco**

Kennwort: **password**

Aktivität - Identifizieren der Hackerkategorie

Hackermerkmal	White-Hat	Grey-Hat	Black-Hat
Nachdem Geldautomaten von einem Laptop aus per Fernzugriff gehackt wurden, arbeitete er mit Herstellern von Geldautomaten zusammen, um die gefundenen Sicherheitslücken zu schließen.			
Von meinem Laptop aus überwies ich mit den Kontonummern und PINs der Opfer 10 Million \$ auf mein Bankkonto, nachdem ich die Eingabe der Ziffern durch die Opfer aufgezeichnet hatte.			
Meine Aufgabe ist die Ermittlung von Schwachstellen im Computersystem meines Unternehmens.			
Ich verwendete Malware, um in mehrere Unternehmenssysteme einzudringen und Kreditkarteninformationen zu stehlen, und verkaufte diese Informationen an den Höchstbietenden.			
Während einer Untersuchung von Sicherheitsschwachstellen stolperte ich über eine Sicherheitslücke in einem Unternehmensnetzwerk, für das ich zugangsberechtigt bin.			
Ich arbeite bei Technologiefirmen, um einen Mangel bei DNS zu beheben.			

Aktivität - Identifizieren der Hackerkategorie

Hackermerkmal	White-Hat	Grey-Hat	Black-Hat
Nachdem Geldautomaten von einem Laptop aus per Fernzugriff gehackt wurden, arbeitete er mit Herstellern von Geldautomaten zusammen, um die gefundenen Sicherheitslücken zu schließen.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Von meinem Laptop aus überwies ich mit den Kontonummern und PINs der Opfer 10 Million \$ auf mein Bankkonto, nachdem ich die Eingabe der Ziffern durch die Opfer aufgezeichnet hatte.	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Meine Aufgabe ist die Ermittlung von Schwachstellen im Computersystem meines Unternehmens.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich verwendete Malware, um in mehrere Unternehmenssysteme einzudringen und Kreditkarteninformationen zu stehlen, und verkaufte diese Informationen an den Höchstbietenden.	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Während einer Untersuchung von Sicherheitsschwachstellen stolperte ich über eine Sicherheitslücke in einem Unternehmensnetzwerk, für das ich zugangsberechtigt bin.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Ich arbeite bei Technologiefirmen, um einen Mangel bei DNS zu beheben.	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>

Aktivität - Identifizieren der Hackerkategorie

Hackermerkmal	White-Hat	Grey-Hat	Black-Hat
Nachdem Geldautomaten von einem Laptop aus per Fernzugriff gehackt wurden, arbeitete er mit Herstellern von Geldautomaten zusammen, um die gefundenen Sicherheitslücken zu schließen.	✗		
Von meinem Unternehmen wurde ich Opfer einer Diebstahlaktion. Ich habe 10 Millionen \$ an Schaden erlitten. Ich bin bereit, das Opfer aufzugeben.			✓
Meine Aufgabe ist es, die Sicherheit meines Unternehmens zu gewährleisten.	✓		
Ich verwende meine Fähigkeiten, um die Sicherheit von Unternehmen zu gewährleisten. Ich habe die Kreditkartennummer eines Kunden gefunden und habe den Höchstbetrag für den Kauf von Waren erhalten.		✗	
Während einer Sicherheitsüberprüfung habe ich eine Sicherheitslücke in einem System gefunden. Ich bin bereit, das Opfer aufzugeben.	✓		
Ich arbeite bei Technologiefirmen, um einen Mangel bei DNS zu beheben.	✓		

Falsch ✗

Sie haben den Hackertypus basierend auf den angegebenen Merkmalen nicht erfolgreich identifiziert. Klicken Sie auf „Zurücksetzen“, um es erneut zu versuchen.

Aktivität - Identifizieren der Hackerkategorie

Hackermerkmal

White-Hat

Grey-Hat

Black-Hat

Nachdem Geldautomaten von einem Laptop aus per Fernzugriff gehackt wurden, arbeitete er mit Herstellern von Geldautomaten zusammen, um die gefundenen Sicherheitslücken zu schließen.
Vorher hatte er für einen Kunden 10 Millionen \$ an Schadensersatz für Opfer aufgezogen.



Sie haben den Hackertypus basierend auf den angegebenen Merkmalen nicht erfolgreich identifiziert. Können Sie die "Zurück"-Taste verwenden, um die Merkmale zu ändern und die Aufgabe neu zu lösen.



Ich arbeite bei Technologiefirmen, um einen Mangel bei DNS zu beheben.

Ups – vielleicht doch eine Instruktorenschulung sinnvoll?



Übung – Wem gehören Ihre Daten?

Zielsetzung

Untersuchen, wem Ihre Daten gehören, wenn diese nicht in einem lokalen System gespeichert sind

Teil 1: Lesen der Nutzungsbedingungen

Teil 2: Wissen Sie, wofür Sie sich registriert haben?

Hintergrund/Szenario

Social Media und Online-Speicher sind inzwischen ein zentraler Lebensbestandteil vieler Menschen. Dateien, Fotos und Videos werden mit Freunden und Familienmitgliedern geteilt. Online-Zusammenarbeit und Besprechungen mit Personen, die viele Kilometer entfernt sind, gehören in Unternehmen zum Alltag. Die Speicherung von Daten ist nicht mehr auf die lokal verfügbaren Geräte beschränkt. Der geografische Standort von Speichergeräten stellt keine Einschränkung für die Speicherung oder Sicherung Ihrer Daten an Außenstellen mehr dar.

Diese Übung befasst sich mit den Nutzungsbedingungen der verschiedenen Online-Dienste. Außerdem erfahren Sie, wie Sie Ihre Daten schützen können.

Erforderliche Ressourcen

- PC oder Mobilgerät mit Internetzugang

Teil 1: Lesen der Nutzungsbedingungen

Wenn Sie Online-Dienste nutzen, um Daten zu speichern oder mit Ihren Freunden und Familienmitgliedern zu kommunizieren, haben Sie vermutlich eine Vereinbarung mit dem Anbieter abgeschlossen. Die Nutzungsbedingungen oder auch allgemeinen Geschäftsbedingungen sind ein rechtlich bindender Vertrag, der die Regeln der Beziehung zwischen Ihnen, dem Anbieter und anderen Benutzern des Dienstes enthält.

Navigieren Sie zur Website eines Online-Dienstes, den Sie nutzen, und suchen Sie nach der Vereinbarung mit den Nutzungsbedingungen. Hier finden Sie eine Liste mit beliebten Social Media und Online-Speicherdiensten.

Lab-Übung mit Fokus auf...

- Facebook
- iCloud
- Dropbox
- OneDrive
- Twitter

Teil 2: Wissen Sie, wofür Sie sich registriert haben?

Wissen Sie wirklich, wofür Sie sich registriert haben, wenn Sie ein Konto erstellt und den Nutzungsbedingungen zugestimmt haben?

In Teil 2 erfahren Sie, wie die Nutzungsbedingungen ausgelegt und von den Anbietern genutzt werden können.

Suchen Sie im Internet nach Informationen zur Auslegung der Nutzungsbedingungen.

Hier finden Sie einige Beispielartikel für den Anfang:

Facebook:

<http://www.telegraph.co.uk/technology/social-media/9780565/Facebook-terms-and-conditions-why-you-dont-own-your-online-life.html>

iCloud:

http://www.americanbar.org/publications/law_practice_today_home/law_practice_today_archive/april12/have-attorneys-read-the-icloud-terms-and-conditions.html

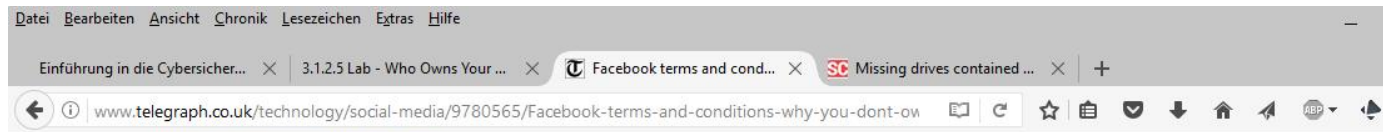
Dropbox:

<http://www.legalgenealogist.com/blog/2014/02/24/terms-of-use-change-dropbox/>

Lesen Sie die Artikel, und beantworten Sie die folgenden Fragen.

a. Wie können Sie sich schützen?

Rechercheauftrag
und zusätzliche
Links auf
Onlineartikel
(auf Englisch)



HOME » TECHNOLOGY » SOCIAL MEDIA

Facebook terms and conditions: why you don't own your online life

Did you read the terms when you joined Facebook, Twitter or LinkedIn? Oliver Smith explains how social networks effectively own your online content.



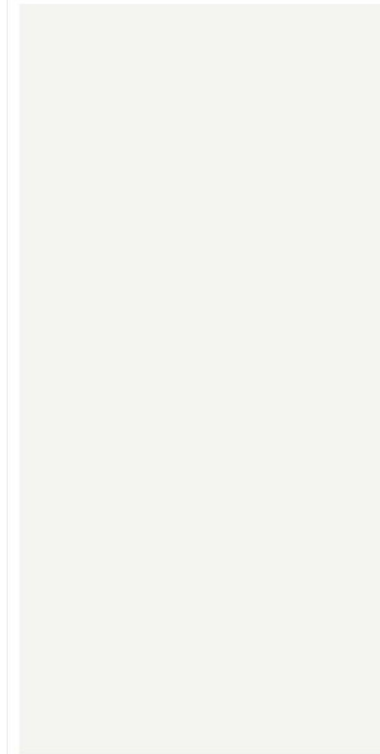
Facebook has something up its sleeve for today. Photo: AP

By Oliver Smith
1:20PM GMT 04 Jan 2013

When joining a social network, you are likely to spend more time considering which photo you will use on your profile than reading the lengthy terms of service document. And yet, off-putting though Facebook's 14,000-word terms of service and data use policy might be, it is a legal contract between you and the social network. Do you know what you've signed up for?

Print this article

Social Media
Technology »
Facebook » Twitter »
Technology News »



Top Technology Videos»



Rise of a tech giant: the history of Google



The history of Uber



Nmap-Port-Scan-Ergebnisse

```

nmap -T4 -A -v 192.168.3.61
Nmap scan report for 192.168.3.61
Host is up (0.0019s latency).
Not shown: 697 closed ports
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 6.7p1 Raspbian 5 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 d5:7e:2f:05:9c:ec:36:43:6c:88:a4:90:dd:5d:48:43 (DSA)
|_ 2048 59:16:3e:41:9b:ac:39:9c:9a:58:ee:a5:ad:b4:3f:4b (RSA)
|_ 256  88:f1:81:b3:fb:4d:15:57:cd:a2:52:a7:fc:b0:1a:15 (ECDSA)
80/tcp    open  http           Apache httpd 2.4.18 ((Raspbian))
|_ http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: Apache/2.4.18 (Raspbian)
|_ http-title: Apache2 Debian Default Page: It works
3389/tcp  open  ms-wbt-server xrdp
|_ MAC Address: 88:27:E8:77:E3:EB (Raspberrry Pi Foundation)
|_ Device type: generic network
|_ Running: Linux 3.X|4.X
|_ OS type: cpe:/o:linux:linux_kernel:s cpe:/o:linux:linux_kernel:4
|_ OS details: Linux 3.2 - 4.0
|_ Uptime guess: 6.004 days (since Tue Mar 01 09:52:48 2016)
|_ Network Distance: 1 hop
|_ TCP Sequence Prediction: Difficulty=261 (Good luck!)
|_ IP ID Sequence Generation: All zeros
|_ Service Info: OS: Linux; CPE: o:linux:linux_kernel

TRACEROUTE
HOP RTT ADDRESS
1 1.90 ms 192.168.3.61

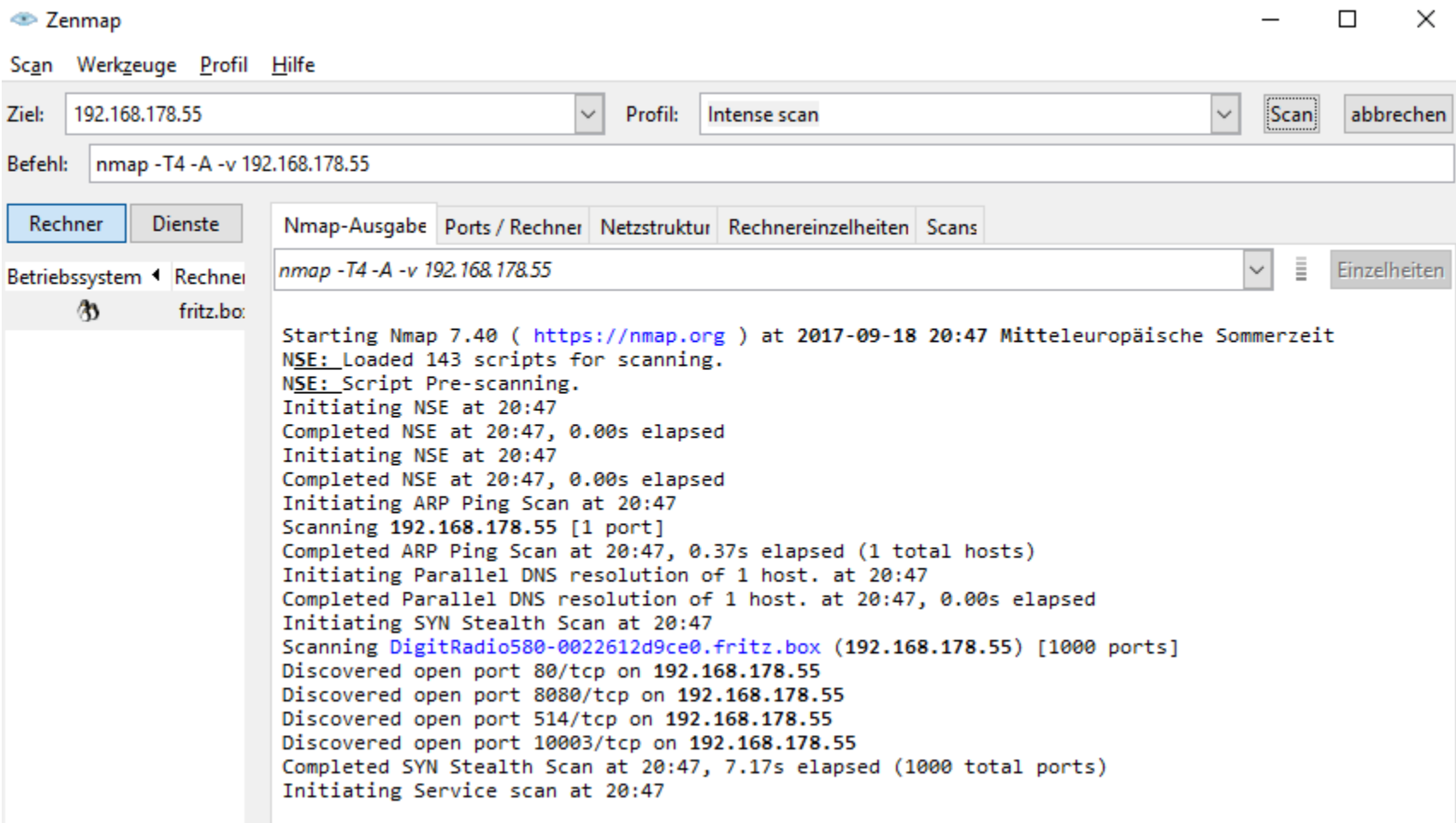
NSE: Script Post-scanning.
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
Initiating NSE at 09:58
Completed NSE at 09:58, 0.00s elapsed
    
```

Scannen von Ports

Das Scannen von Ports ist ein Prozess zum Testen eines Computers, Servers oder anderer Netzwerkhosts auf offene Ports. In Netzwerken wird jeder Anwendung, die auf einem Gerät ausgeführt wird, eine Kennung zugewiesen, die als Portnummer bezeichnet wird. Diese Portnummer wird an beiden Enden einer Übertragung verwendet, damit die richtigen Daten an die richtige Anwendung übergeben werden. Das Scannen der Ports kann auch aus böswilliger Absicht durch ein Ausspähtool zum Ermitteln des Betriebssystems und der Services durchgeführt werden, die auf einem Computer oder Host ausgeführt werden. Es kann aber auch ohne böse Absicht von einem Netzwerkadministrator zum Überprüfen der Sicherheitsrichtlinien in einem Netzwerk verwendet werden.

Wenn Sie die Sicherheit der Firewall und der Ports in Ihrem eigenen Computer-Netzwerk analysieren möchten, können Sie mit einem Tool zum Scannen der Ports, wie zum Beispiel Nmap, alle offenen Ports im Netzwerk suchen. Das Scannen von Ports kann die Vorstufe eines Netzwerkangriffs sein und sollte deswegen nicht ohne Genehmigung für öffentliche Server im Internet oder in einem Unternehmensnetzwerk durchgeführt werden.

... motiviert zum weiterarbeiten und ausprobieren.
Aber : im gesetzlichen Rahmen!



Zenmap

Scan Werkzeuge Profil Hilfe

Ziel: 192.168.178.55 Profil: Intense scan Scan abbrechen

Befehl: nmap -T4 -A -v 192.168.178.55

Rechner Dienste

Betriebssystem Rechner

fritz.bo:

Nmap-Ausgabe Ports / Rechner Netzstruktur Rechnereinheiten Scans

`nmap -T4 -A -v 192.168.178.55` Einzelheiten

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-09-18 20:47 Mitteleuropäische Sommerzeit
NSE: Loaded 143 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:47
Completed NSE at 20:47, 0.00s elapsed
Initiating NSE at 20:47
Completed NSE at 20:47, 0.00s elapsed
Initiating ARP Ping Scan at 20:47
Scanning 192.168.178.55 [1 port]
Completed ARP Ping Scan at 20:47, 0.37s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:47
Completed Parallel DNS resolution of 1 host. at 20:47, 0.00s elapsed
Initiating SYN Stealth Scan at 20:47
Scanning DigitRadio580-0022612d9ce0.fritz.box (192.168.178.55) [1000 ports]
Discovered open port 80/tcp on 192.168.178.55
Discovered open port 8080/tcp on 192.168.178.55
Discovered open port 514/tcp on 192.168.178.55
Discovered open port 10003/tcp on 192.168.178.55
Completed SYN Stealth Scan at 20:47, 7.17s elapsed (1000 total ports)
Initiating Service scan at 20:47
```

- Informative Texte und ansprechende Abbildungen
- Lab-Übungen – Anleitungen liegen als PDF-Dateien vor
- Recherche Übungen
- Videos

GuT Workshop Agenda



- IT Sicherheit als TOP Thema im Wahljahr
- IT Sicherheit im Unterricht am Berufskolleg
- Netacad Cybersecurity „Introduction“ oder „Essentials“
- Einstiegshürden
- Beispiele für Lernmaterial im Kurs
- ➔ Didaktische Überlegungen und Lernsituationen
- Fragen?

Fallstudie IT-Sicherheit 2

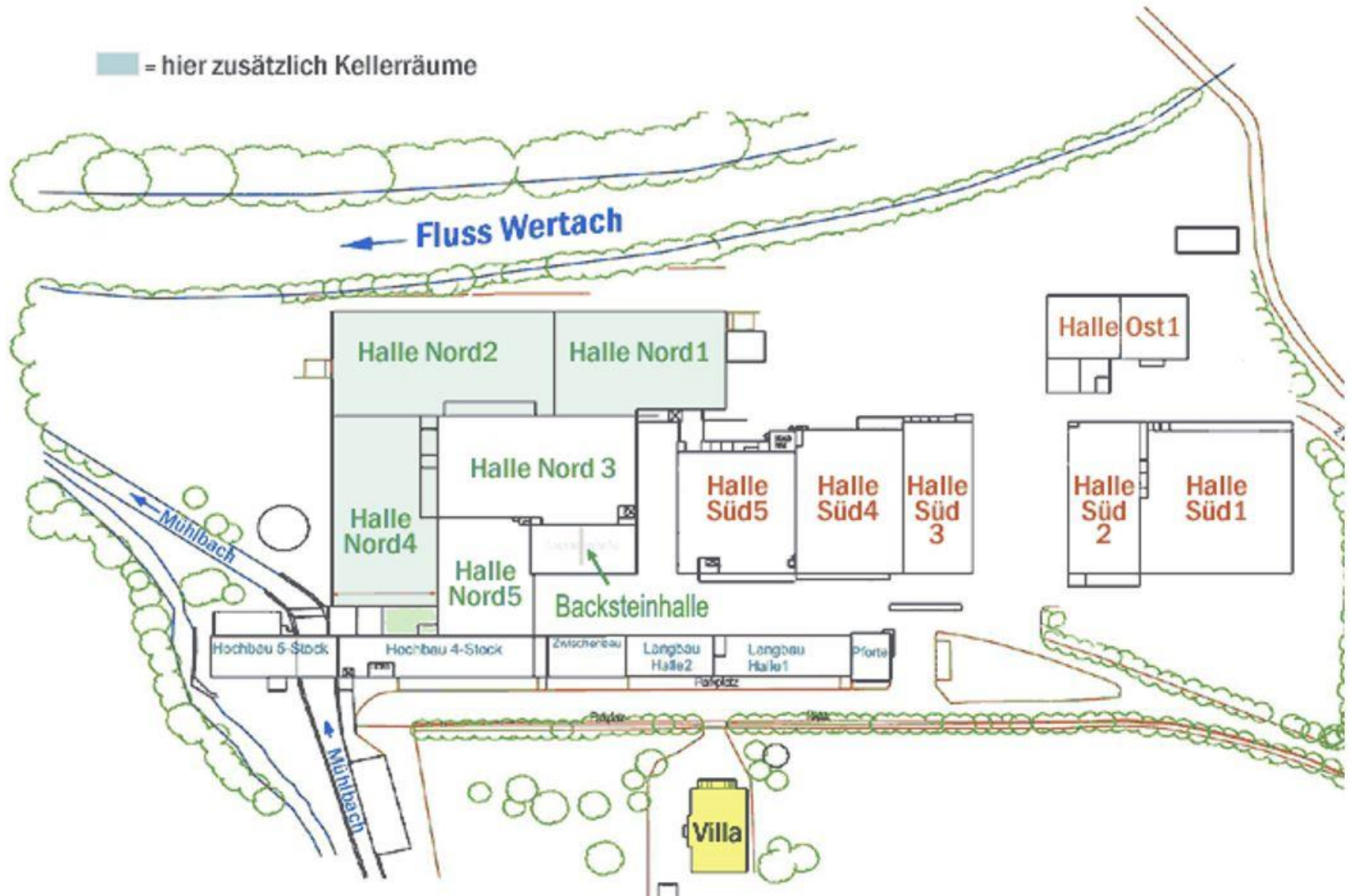
TrotProt GmbH ist ein mittelständisches Unternehmen, produziert Kinderspielzeuge der neuesten Generation. Aufgrund der sehr guten geschäftlichen Lage überlegt die Firmenleitung, den Firmenstandort und die Produktion zu verlagern und die in der Abbildung grün beschrifteten Hallen und den „Hochbau 4-Stock“ in einem Gewerbepark anzumieten.

Es ist zu prüfen, inwieweit das Unternehmen in dem Hallen und dem Verwaltungsgelände sinnvoll untergebracht werden kann. Dazu gilt es zunächst folgende Planungsphasen zu durchlaufen:

- I. Phase Netzwerkplanung
- II. Phase Sicherheitsplanung



Pforte mit Langbau



Im Rahmen der Vernetzungsplanung sind folgende Vorgaben zu beachten:

- in jeder Halle sind 8 Windows 7 Rechner mit dem Rechenzentrum in der „Backsteinhalle“ zu vernetzen, in jeder Halle gibt es einen Netzwerkdrucker
- die Verwaltung ist im „Hochbau 4-Stock“ untergebracht und hat 20 Rechner im Verwaltungsnetz, 4 Rechner im Produktionsnetz und 4 Netzwerkdrucker (2 in jedem Netz)
- zentraler Internetzugang (100 MBit/s) ist in der „Backsteinhalle“ vorhanden
- Halle Nord 5 ist zentrales Lager mit WLAN

Die Daten zwischen Verwaltungs- und Produktionsnetz sollen durch eine sichere eMail-Kommunikation ausgetauscht werden. Die Netze sollen voneinander getrennt sein.

Im Rahmen der Sicherheitsplanung soll eine „Security in Depth“-Strategie durchgeführt werden und die IT der Firma gegen mögliche Sicherheitsrisiken geschützt werden.

Haben Sie Fragen?

Vielen Dank für Ihre Aufmerksamkeit!