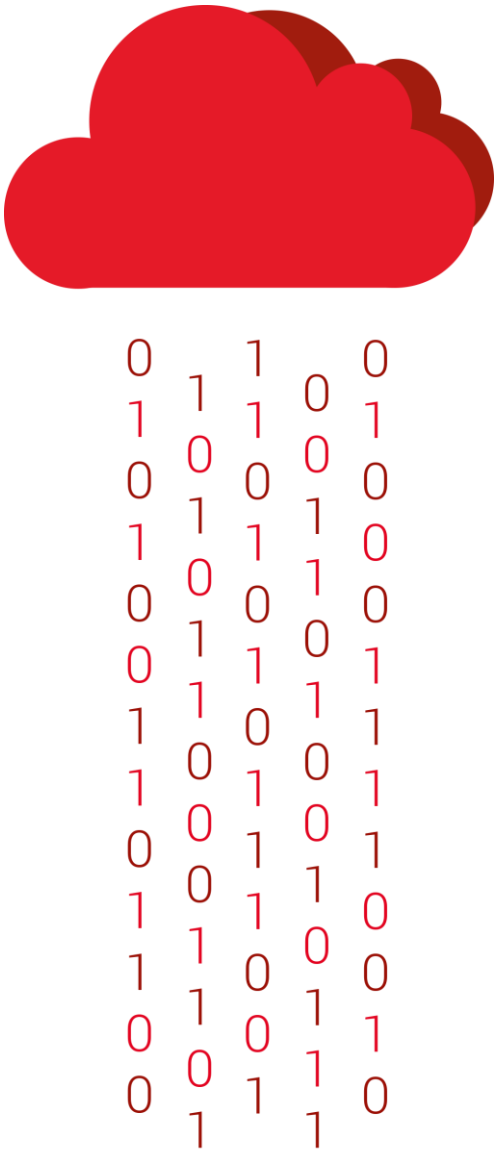
Cyber Security Workshop



Patrick Eisoldt

- Studium an der Hochschule Albstadt-Sigmaringen und der Glyndwr University in Wales
- Praktika/Thesen: Siemens, Marquardt
- November 2010 bis August 2011: Mitarbeiter Digitale Forensik
- Seit 2012: Wissenschaftlicher Mitarbeiter im Projekt Open C^3S, Hochschule Albstadt-Sigmaringen – IWW

- Schwerpunkte: Digitale Forensik, Windows-Forensik, Python (Forensik und Pen-Tests)

Tobias Scheible

- Studium Kommunikations- und Softwaretechnik, Fachrichtung Kommunikationstechnik, Hochschule Albstadt-Sigmaringen
- 2009 bis 2012: Softwareingenieur im Bereich Web Development, Gute Aussicht Kommunikations GmbH
- Seit 2012: Wissenschaftlicher Mitarbeiter im Projekt Open C^3S, Hochschule Albstadt-Sigmaringen – IWW

- Schwerpunkte: Internet Technologien, Frontend Development, Web Vulnerability Scans und Cloud Computing

Cyber Security Workshop

- Die Ziele des Workshops:
  - Hintergründe von Angriffen verstehen
  - Methoden der Angreifer nachvollziehen
  - Bewusstsein für Sicherheitslücken bekommen

- Inhalte des Workshops:
  - Beispiele in vielen Themengebieten
  - Viele Aufgaben, die selbst ausprobiert werden können

Vorstellungsrunde

- Wie heißt ihr und woher kommt ihr?
- Studiert ihr oder wo arbeitet ihr?
- Habt ihr bereits Erfahrungen im Bereich Cyber Security?
- Was ist eure Motivation für die Teilnahme am Workshop?

- Was sind eure Wünsche oder Erwartungen an den Workshop?

Workshop Agenda

- 1. Cyber Security
- 2. System Security
- 3. Network Security
- 4. Data Security
- 5. Web Security
- 6. Cyber Defense

1. Cyber Security

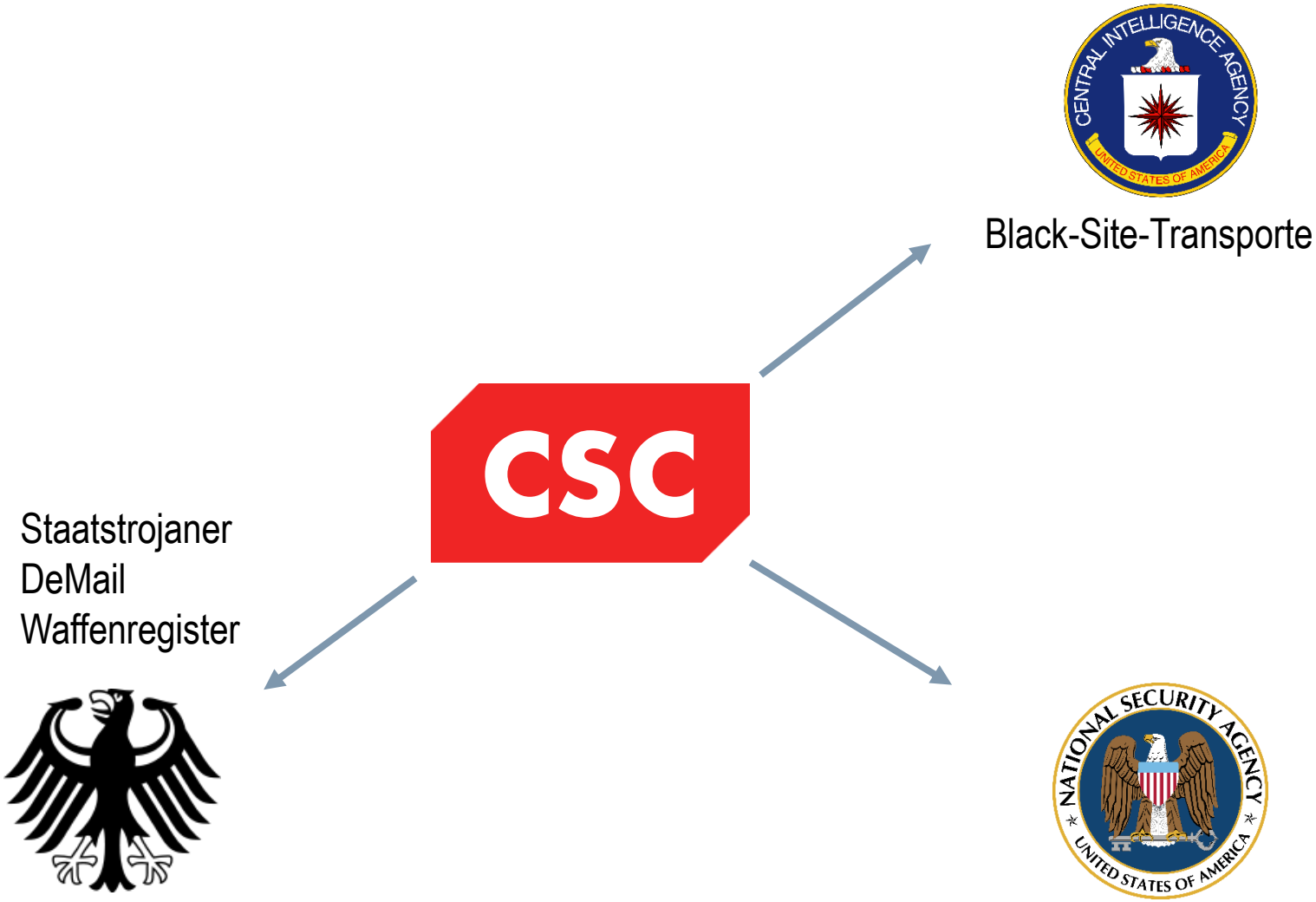
Workshop Agenda

- 1. Cyber Security
  - » Bedeutung von IT-Sicherheit
  - » Sicherheit in der Praxis
  - » Analyse von Stuxnet
- 2. System Security
- 3. Network Security
- 4. Data Security
- 5. Web Security
- 6. Cyber Defense

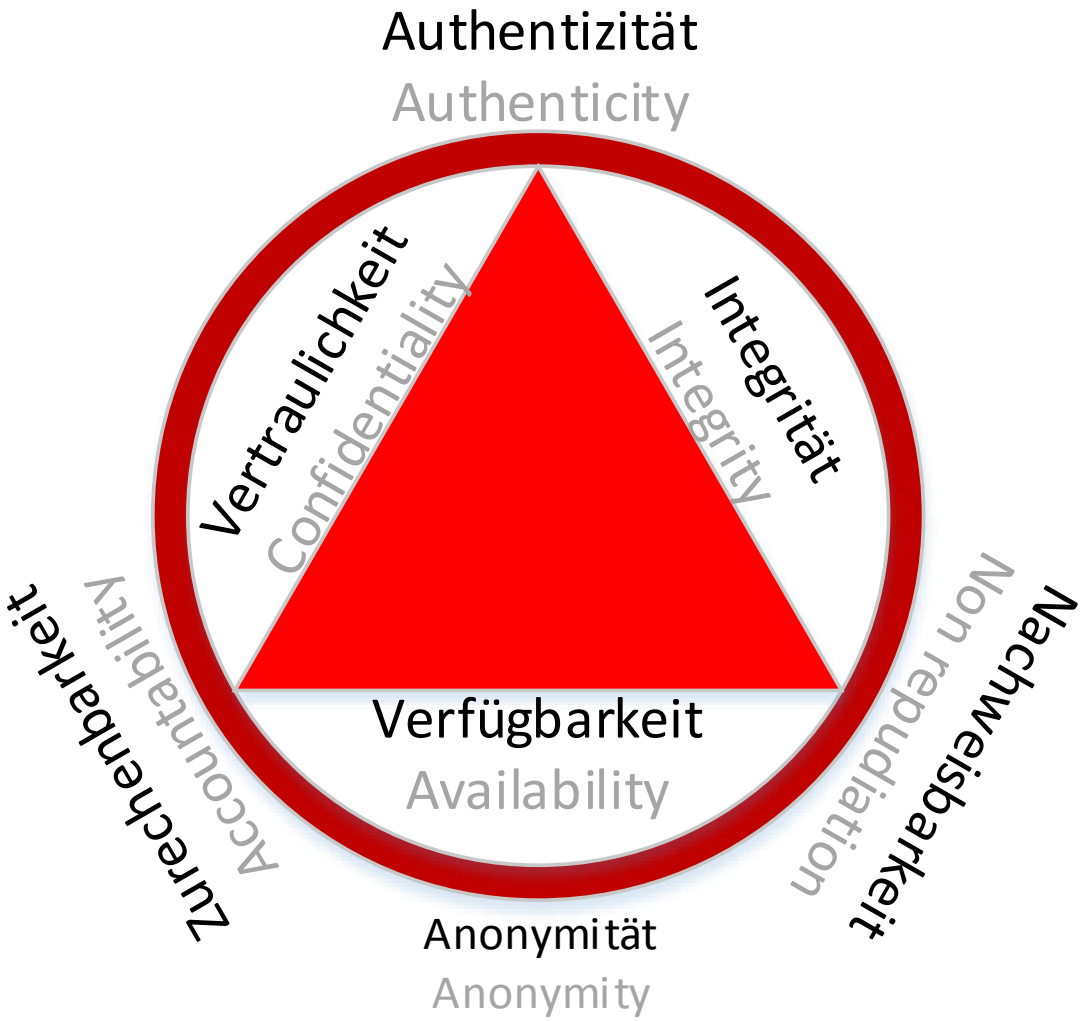
Bedeutung von IT-Sicherheit

- „Hacker haben Berichten zufolge das gesamte Computersystem von Sony Pictures lahmgelegt. Zudem soll Sonys Play-Store-Konto gehackt worden sein.“ golem.de 14.11.2014
- „Der Trojaner Regin soll ähnlich wie der Computerwurm Stuxnet im großen Stil Industriespionage betrieben haben. Betroffen sind davon vor allem Russland und Saudi-Arabien.“ zeit.de 24.11.2014
- „Britische und US-amerikanische Geheimdienste sollen mit der Spionagesoftware Regin den massiven Cyberangriff auf Belgacom und EU-Behörden ausgeführt haben. Die Malware kann auch Mobilfunk-Stationen überwachen.“ heise.de 25.11.2014

IT-Beratungs- und -Dienstleistungsunternehmen



Bedeutung von IT-Sicherheit



Bedeutung von IT-Sicherheit

- Vertraulichkeit
  - » Informationen sind für Unbefugte unzugänglich und vor Missbrauch geschützt
- Integrität
  - » Unbemerkte Veränderungen an Informationen sind nicht möglich
- Verfügbarkeit
  - » Informationen müssen verfügbar sein

Bedeutung von IT-Sicherheit

- Authentizität
  - » Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit einer Information
- Nachweisbarkeit
  - » Kein unzulässiges Abstreiten durchgeführter Handlungen
- Zurechenbarkeit
  - » Ein Handlung kann einer Person eindeutig zugeordnet werden
- Anonymität
  - » Zuordnung von personenbezogenen Daten ist nicht mehr möglich

Sicherheit in der Praxis

00000000

?

Sicherheit in der Praxis

00000000

Launch-Code für die in den USA stationierten Atomraketen

Quelle: heise.de

Sicherheit in der Praxis

Quelle: chip.de

Fingerabdruckscanner

Quelle: rolf-fensterbau.de

Fingerabdruckscanner

Quelle: aivanet.com

Fingerabdruckscanner

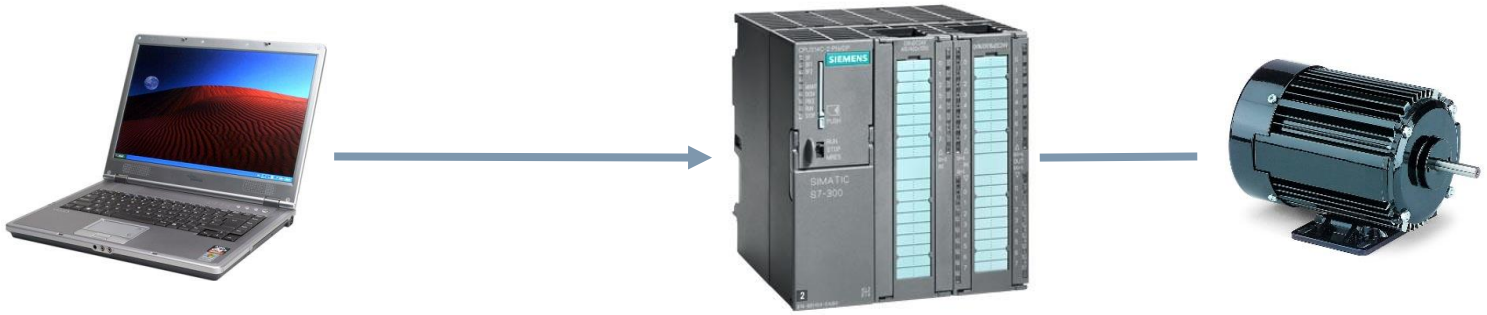
Quelle: telegraph.co.uk

Fingerabdruckscanner

- Einmal verlorener Abdruck kann nicht ersetzt werden
- Nur „10“ Möglichkeiten stehen zur Verfügung
- Größere Verbreitung sorgt für häufigere Diebstähle
- Komplexe Lösung nicht immer die sicherste

Stuxnet: Allgemeine Infos

- Typ: Computerwurm
- Beginn: November 2007
- Entdeckung: Juni 2010
- Entwicklungszeit: > 6 Monate bei 5 – 10 Entwicklern
- Infektionsweg: USB-Speichermedien, LAN
- Angriffsziel: Industrieanlagen (Siemens Simatic S7)
  - » Frequenzumrichter (Steuerung für Motorgeschwindigkeit)



Stuxnet: Angriffsweise

1. Stuxnet wird durch ein USB-Speichermedium in das LAN einer Firma eingeschleust
2. Verbreitung über das LAN
3. Lokalisierung des Field-PG (Programmiergerät für SPS)
4. Infizierung des Field-PG (Projektordner und Bibliotheken)
5. Manipulation der SPS-Software bei Aktualisierung

Resultat: Unerwartetes Verhalten des Frequenzumrichters

Optional: Aktualisierung über P2P

Optional: Kommunikation mit C&C-Server

Stuxnet: Architektur

- Ein Programm dient als Hülle für die Komponenten
  - » Eine große DLL und zwei verschlüsselte Container
- Wenn der Wurm aktiv wird, entpackt die Hülle die DLL-Datei und verknüpft sie mit dem Arbeitsspeicher
- DLL verfügt über eine Exporttabelle (Liste aller Funktionen)

Stuxnet: Speicherdump-Analyse

2. System Security

Workshop Agenda

- 1. Cyber Security
- 2. System Security
  - » Passwörter knacken
  - » Sichere Passwörter
  - » Windows Forensik
- 3. Network Security
- 4. Data Security
- 5. Web Security
- 6. Cyber Defense

Passwörter knacken

- PDF-Passwortschutz
  - » Die Stärke des Schutzes ist abhängig von der verwendeten Technik
  - » Die Länge des Passwortes ist häufig entscheidend

- Praxis 2.1: PDF Passwörter knacken

Sichere Passwörter

- Angriffe auf Passwörter
  - » Wörterbuchangriff
  - » Bekannte Ersetzungsmethoden
  - » Brute force
- Eselsbrücken
  - » 3 beliebige Wörter (Vorteil: Smartphone u. Tablet)
  - » Anfangsbuchstaben eines willkürlichen Satzes + Sonderzeichen
  - » Tipp: Dialekt verwenden

- Praxis 2.2: Sicheres Passwort aus Büchern

Sichere Passwörter

- Wie sieht ein sicheres Passwort aus?
  - » Mindestens 10 Zeichen
  - » Neben Groß- und Kleinbuchstaben auch Umlaute und Sonderzeichen
  - » Keine Begriffe aus Wörterbüchern

- Praxis 2.3: Passwortkarten

Passwortkarten

Nr: Kategorie:

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1										
2										
3										
4										
5										
6										
7										
8										

Passwortkarten

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	ld	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort:

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de Passwort: V=

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de

Passwort: V=6<

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de

Passwort: V=6<Bd

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de

Passwort: V=6<BdG2

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Passwortkarten

Link: sparkasse.de

Passwort: V=6<BdG2W-

Nr: 1 Kategorie: Online-Banking

	abc	def	ghi	jkl	mno	pqr	stu	vwx	yz	#
1	x!	Q*	S<	bL	Pn	X:	V=	dd	n3	9K
2	T8	wb	eT	98	C,	6<	ff	aO	X>	Hm
3	Bd	dD	C)	7c	gz	er	q]	p=	t&	1P
4	ne	a@	e-	W8	k-	G2	>d	PE	z3	z:
5	V·	H>	d*	W-	Wl	J8	Qi	U,	Id	7R
6	5=	mF	2n	XY	m:	f<	YH	mo	h4	7-
7	vT	ej	R:	+<	Vg	Nh	a9	6;	dJ	N{
8	d6	G7	p)	ek	pJ	mb	y2	e?	Jm	Rv

Windows Forensik

- Anwendungsdaten sind frei zugänglich und können dank einheitlicher Datenverwaltung einfach extrahiert werden.
- Z. B. SQLite: Firefox, Chrome, Skype, … (auch Mac: Safari, Mail)
- Pfad zu den Anwendungsdaten: C:\Users\[Benutzer]\AppData\Roaming oder %APPDATA%

- Praxis 2.4: Daten analysieren

3. Network Security

Workshop Agenda

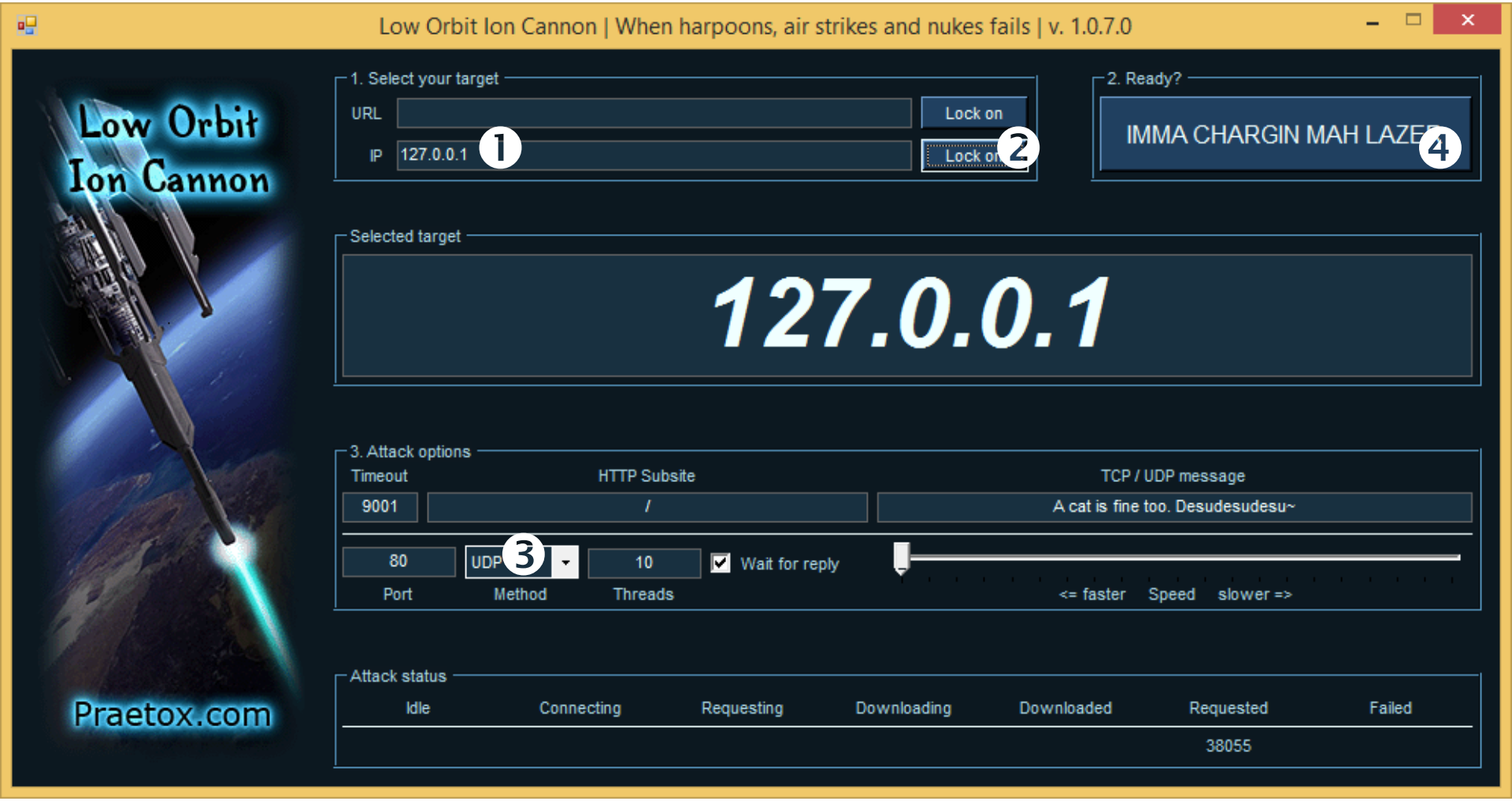
- 1. Cyber Security
- 2. System Security
- 3. Network Security
  - » Angriffe über das Netzwerk
  - » Google Webcam Hacks
- 4. Data Security
- 5. Web Security
- 6. Cyber Defense

Angriffe über das Netzwerk

- (Distributed) Denial of Service Attack
- Eine größere Anzahl von Anfragen können nicht verarbeitet werden und führen zu einer Nichtverfügbarkeit eines Dienstes

- Praxis 3.1: (D)DOS-Angriff

Angriffe über das Netzwerk



Google Webcam Hacks #1

- Google kann auch nach URLS und Seitentitel suchen
- Beispiel Suchanfragen:
  - inurl:"viewerframe?mode=motion"
  - intitle:"snc-rz30 home"
  - intitle:"WJ-NT104 Main"
  - inurl:LvAppl intitle:liveapplet
  - intitle:"Live View / - AXIS"
  - inurl:indexFrame.shtml

- Praxis 3.2: Suche nach Webcams bei Google

4. Data Security

Workshop Agenda

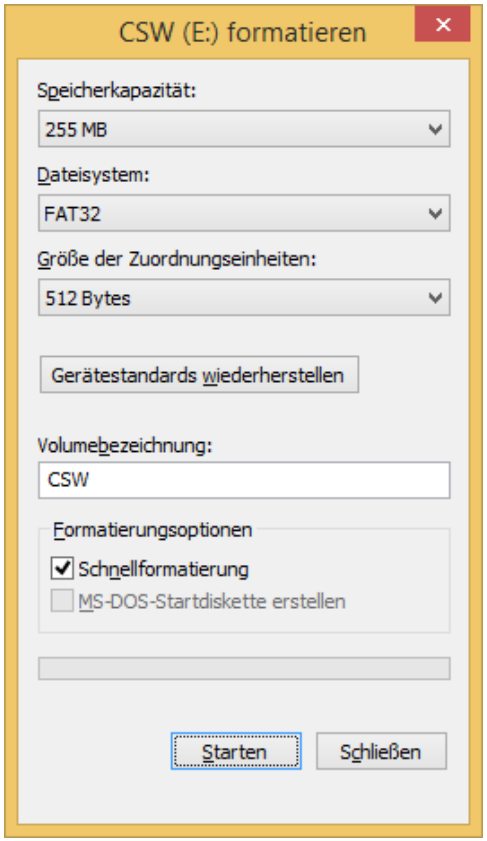
- 1. Cyber Security
- 2. System Security
- 3. Network Security
- 4. Data Security
  - » Gelöschte Daten wiederherstellen
  - » Daten sicher löschen
  - » Daten verschlüsseln
- 5. Web Security
- 6. Cyber Defense

Gelöschte Daten wiederherstellen

- Wie arbeitet ein Dateisystem?
  - » Vergleich: Festplatte = Enzyklopädie (unsortiert)
  - » Zentrales Dateiverzeichnis = Inhaltsverzeichnis der Enzyklopädie
  - » Dateiverzeichnis enthält verschiedene Attribute (z. B. Verweis auf Speicherort)
  - » Eintrag gelöscht -> Datei „unauffindbar“
  - » Carving

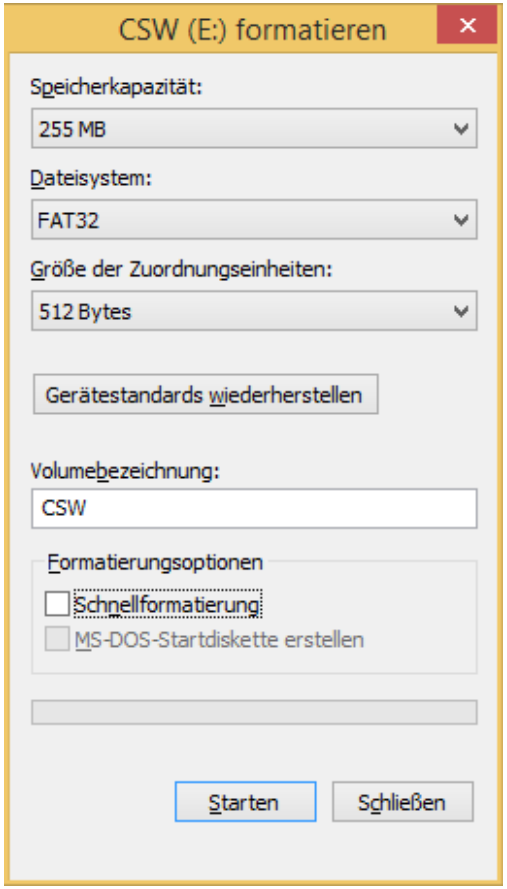
- Praxis 4.1: Daten mit Recuva wiederherstellen

Gelöschte Daten wiederherstellen



- Praxis 4.1: Daten mit Recuva wiederherstellen

Daten sicher löschen



- Praxis 4.2: Daten sicher löschen durch Normalformatierung

Daten sicher löschen

- Unterschied zwischen den Formatierungsarten:
- *Schnellformatierung*
  - » *Dateien werden aus dem Inhaltsverzeichnis entfernt. Eine Suche nach fehlerhaften Sektoren wird nicht durchgeführt.*
- *Normalformatierung*
  - » Eine Suche nach fehlerhaften Sektoren wird durchgeführt. Anschließend findet die Löschung der vorhandenen Dateien durch Überschreibung statt.

Daten sicher löschen

- Eraser
  - » Sicheres Löschen unter Windows
  - » Benötigt keine Installation
  - » Daten werden mit Zufallsdaten überschrieben
  - » Windows-Partition kann nicht gelöscht werden

- Praxis 4.3: Daten sicher löschen mit Eraser

Daten verschlüsseln

- 7zip
  - » Schnelle unkomplizierte Verschlüsselung
- TrueCrypt
  - » Etwas aufwendiger
  - » Variante 1: Container
  - » Variante 2: Festplatte mit Bootloader

- Praxis 4.4: Daten mit 7-Zip verschlüsseln
- Praxis 4.5: Daten mit TrueCrypt verschlüsseln

5. Web Security

Workshop Agenda

- 1. Cyber Security
- 2. System Security
- 3. Network Security
- 4. Data Security
- 5. Web Security
  - » Sicher im Internet
  - » Anonym im Internet
  - » Websites manipulieren
- 6. Cyber Defense

Sicher im Internet

- Plugins nur mit Bestätigung ausführen
- Datenschutz Einstellung
- Verfügbare Plugins verstecken
- Nützliche Erweiterungen – Firefox Add-Ons
  - » AdBlock Edge
  - » Random Agent Spoofer
  - » NoScript

  - » Praxis 5.1: Firefox Security-Tuning in vier Schritten

Anonym im Internet

- Proxy
  - Proxy bedeutet Stellvertreter und handelt im Auftrag eines anderen
  - Kann unterschiedliche Netze miteinander verbinden
  - Kann Netzwerk-Daten filtern, optimieren und zwischenspeichern
  - Die tatsächliche IP-Adresse des Nutzers bleibt verborgen
- Virtual Private Network
- Tor Browser

Anonym im Internet

- Proxy
- Virtual Private Network
  - » Ein virtuelles Netzwerk, welches private Daten über ein öffentliches Netzwerk (z.B. über das Internet) verschlüsselt transportiert
  - » Über eine bestehende IP-Verbindung wird eine zweite Verbindung (Tunnel) aufgebaut
  - » Der gesamte Datenverkehr wird über den VPN-Server geleitet
- Tor Browser

Anonym im Internet

- Proxy
- Virtual Private Network
- Tor Browser
  - » Spendenfinanziertes Opensource-Projekt mit über 5000 Tor-Nodes
  - » Komplette Browser Bundles für Windows, Mac OS X, Linux, Android
  - » Zufällige und verschlüsselte Route über drei Tor-Nodes
  - » Jede Note kennt immer nur den Vorgänger und den Nachfolger
  - » Wichtig: nur Anonymisierung, keine Verschlüsselung oder Integritätsschutz

  - » Praxis 5.2: Tor Browser in der Nutzung

Websites manipulieren

- Manipulation über Short-Link
  - » Anfällig bei der Verbreitung über soziale Netzwerke
  - » Auf Smartphones spielt die URL eine untergeordnete Rolle

  - » Praxis 5.3: Manipulation über Short-Link

Social Engineering

- Der Mensch als größtes Sicherheitsrisiko
- Know-how der Mitarbeiter
  - » Passwörter wurden nicht geändert, entsprechen nicht den Vorgaben oder sind offen zugänglich
  - » Umgang mit vertraulichen Informationen in der Öffentlichkeit wie z.B. Flughafen Lounge, Flugzeug, Zug, Restaurant, …
  - » Social Media – Privates und Geschäftliches werden immer mehr vermischt
- Social Engineering, um Menschen gezielt zu manipulieren

Social Engineering

- Hilfsbereitschaft
  - „Ich bin eine neue Studentin, ich muss nur schnell meine E-Mails abrufen.“
  - „Könnten sie mir bitte kurz helfen, ich suche Informationen über ….“
- Autoritätsgläubigkeit
  - „Ich bin ein Professor aus Sigmaringen und muss schnell an den Rechner.“
  - „Ich bin die Sekretärin der Rektorin und brauche heute Abend noch …..“
- Eitelkeit
  - „Ich bin ein Journalist und mache einen Artikel über innovative Studiengänge.“
  - „Ich habe ein großes Problem, nur Sie können mir helfen.“

Social Engineering

- Neugierde
  - Öffnen von Attachments, Klicken auf Links, zufällig gefundene DVDs oder USB-Sticks, kostenlose Software, …
- Einschüchterung
  - Phishing E-Mail: „Wenn Sie nicht Ihr Passwort erneuern, sperren wir Ihren Account.“
- Erpressung
  - Phishing E-Mail: „Wenn Sie nicht Ihr Passwort erneuern, erheben wir eine Gebühr von 15 Euro …“

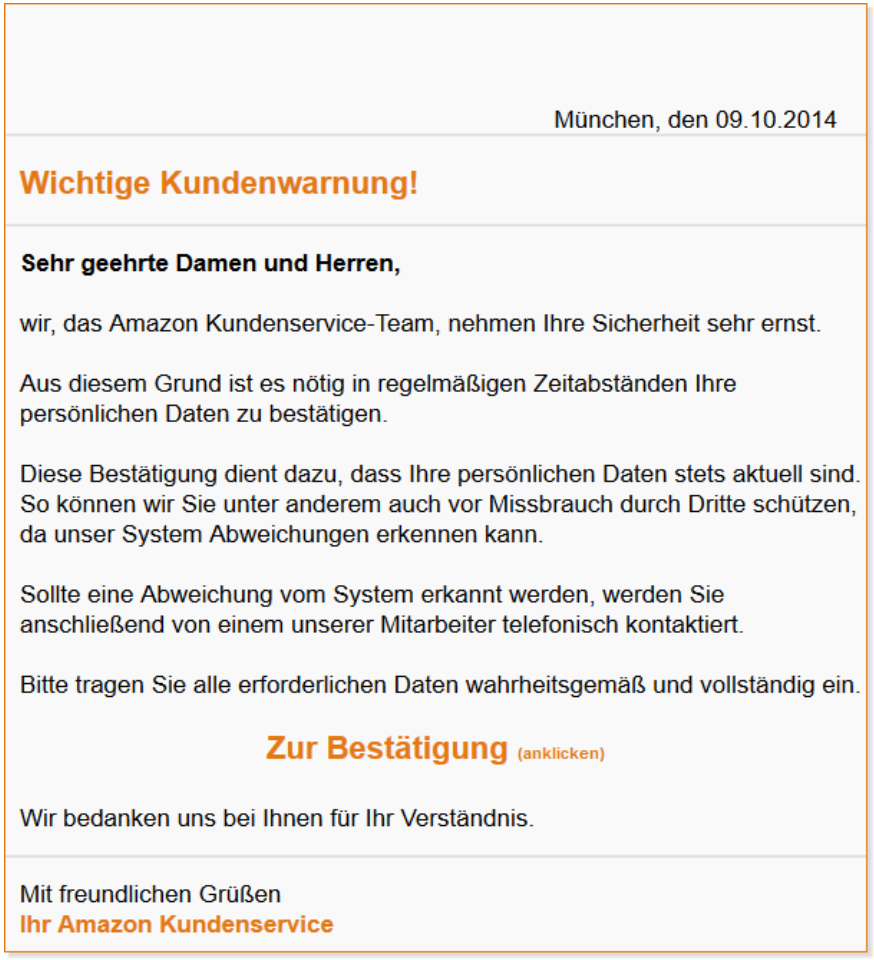
Social Engineering

- Legitimation
  - „Ich habe gerade mit ihrer Kollegin Jessica gesprochen und sie hat gesagt, sie können mir weiterhelfen …“
  - „Ich habe ihren Vorgesetzten, Herrn Müller auf einem Workshop getroffen. Ich weiß, dass er jetzt im Urlaub in Neuseeland ist. Er hat mir versichert, sie können mir helfen …..“
  - „Ich hab vorhin beim Zusammenpacken nach der Präsentation aus Versehen diesen Adapter eingesteckt. Kann ich ihn kurz wieder zurückbringen, ich möchte keinen Ärger bekommen.“
  - „Ich habe gerade eigentlich noch Vorlesung bei Herrn Müller, da ist mein Notebook noch drin, kann ich mal kurz an den Rechner …“

Social Engineering

- Maßnahmen
  - Sensibilisierung und Befähigung der Mitarbeiter
  - Stärken und Schwächen der Mitarbeiter als Tatsache akzeptieren (z.B. Hilfsbereitschaft = Kundenfreundlichkeit)
  - Verhaltensmaßnahmen anbieten und schulen: Ablehnen mit Gegenangebot, Firmenrichtlinie als Verteidigung, ...
  - Aufzeigen und Demonstrationen von möglichen Angriffen
  - Zentrale Position im Unternehmen schaffen, an die „dubiose“ Anfragen weitergegeben werden können

Phishing



München, den 09.10.2014

Wichtige Kundenwarnung!

Sehr geehrte Damen und Herren,

wir, das Amazon Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst.

Aus diesem Grund ist es nötig in regelmäßigen Zeitabständen Ihre persönlichen Daten zu bestätigen.

Diese Bestätigung dient dazu, dass Ihre persönlichen Daten stets aktuell sind. So können wir Sie unter anderem auch vor Missbrauch durch Dritte schützen, da unser System Abweichungen erkennen kann.

Sollte eine Abweichung vom System erkannt werden, werden Sie anschließend von einem unserer Mitarbeiter telefonisch kontaktiert.

Bitte tragen Sie alle erforderlichen Daten wahrheitsgemäß und vollständig ein.

Zur Bestätigung (anklicken)

Wir bedanken uns bei Ihnen für Ihr Verständnis.

Mit freundlichen Grüßen
Ihr Amazon Kundenservice

Amazon EU S.A.R.L., Société à responsabilité limitée, 5 Rue Plaetis, L-2338 Luxemburg

Phishing

München, den 09.10.2014

Wichtige Kundenwarnung!

Sehr geehrte Damen und Herren,

wir, das Amazon Kundenservice-Team, nehmen Ihre Sicherheit sehr ernst.

Aus diesem Grund ist es nötig in regelmäßigen Zeitabständen Ihre persönlichen Daten zu bestätigen.

Diese Bestätigung dient dazu, dass Ihre persönlichen Daten stets aktuell sind. So können wir Sie unter anderem auch vor Missbrauch durch Dritte schützen, da unser System Abweichungen erkennen kann.

Sollte eine Abweichung vom System erkannt werden, werden Sie anschließend von einem unserer Mitarbeiter telefonisch kontaktiert.

Bitte tragen Sie alle erforderlichen Daten wahrheitsgemäß und vollständig ein.

Zur Bestätigung (anklicken)

Wir bedanken uns bei Ihnen für Ihr Verständnis.

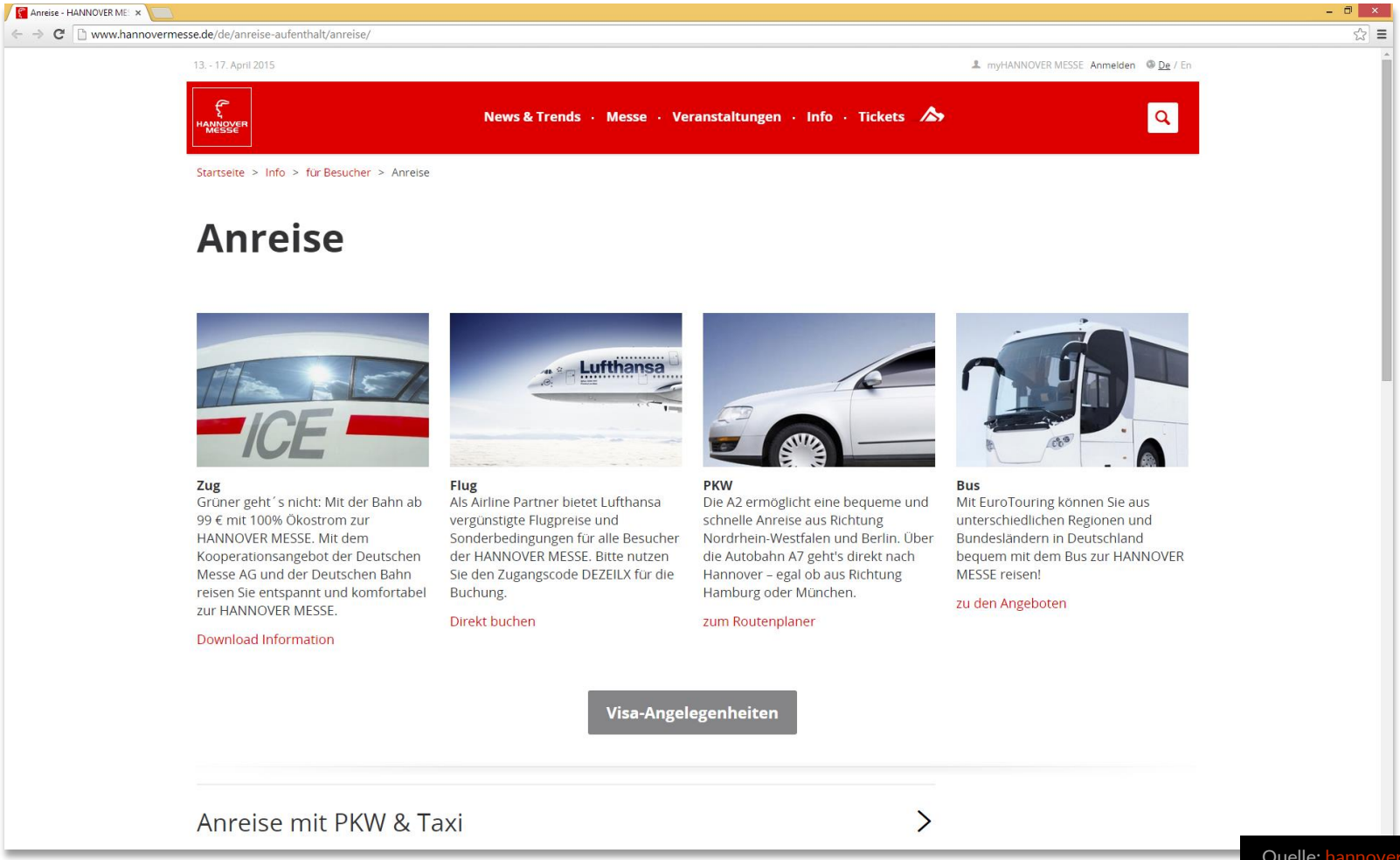
Mit freundlichen Grüßen
Ihr Amazon Kundenservice

Amazon EU S.A.R.L., Société à responsabilité limitée, 5 Rue Plaetis, L-2338 Luxemburg

- 1. Falsche E-Mail Adresse
  - » Nicht bei Amazon registriert
- 2. Keine Anrede
  - » Amazon hat meine Daten
- 3. Kein Amazon Link
  - » http://link-share.cc/10

PHISHING

Phishing | fiktives Szenario



Quelle: hannovermesse.de

Phishing | fiktives Szenario

DB BAHN

Bequem und klimafreundlich zur HANNOVER MESSE 2015 – Das weltweit wichtigste Technologieereignis

Mit der Bahn ab 99 € - deutschlandweit

Mit dem Kooperationsangebot der Deutschen Messe AG und der Deutschen Bahn reisen Sie entspannt und komfortabel zur HANNOVER MESSE 2015.

Ihre An- und Abreise im Fernverkehr der Deutschen Bahn mit dem Veranstaltungsticket wird mit 100% Ökostrom durchgeführt. Die für Ihre Reise benötigte Energie wird ausschließlich aus erneuerbaren Energiequellen bezogen.

Der Preis für Ihr Veranstaltungsticket zur Hin- und Rückfahrt* nach Hannover Messe/Laatzen beträgt:

- **2. Klasse 99,- Euro**
- **1. Klasse 159,- Euro**

Den Ticketpreis für internationale Verbindungen nennen wir Ihnen gerne auf Anfrage.

Die Fahrkarte ist gültig vom 11. April bis 19. April 2015.

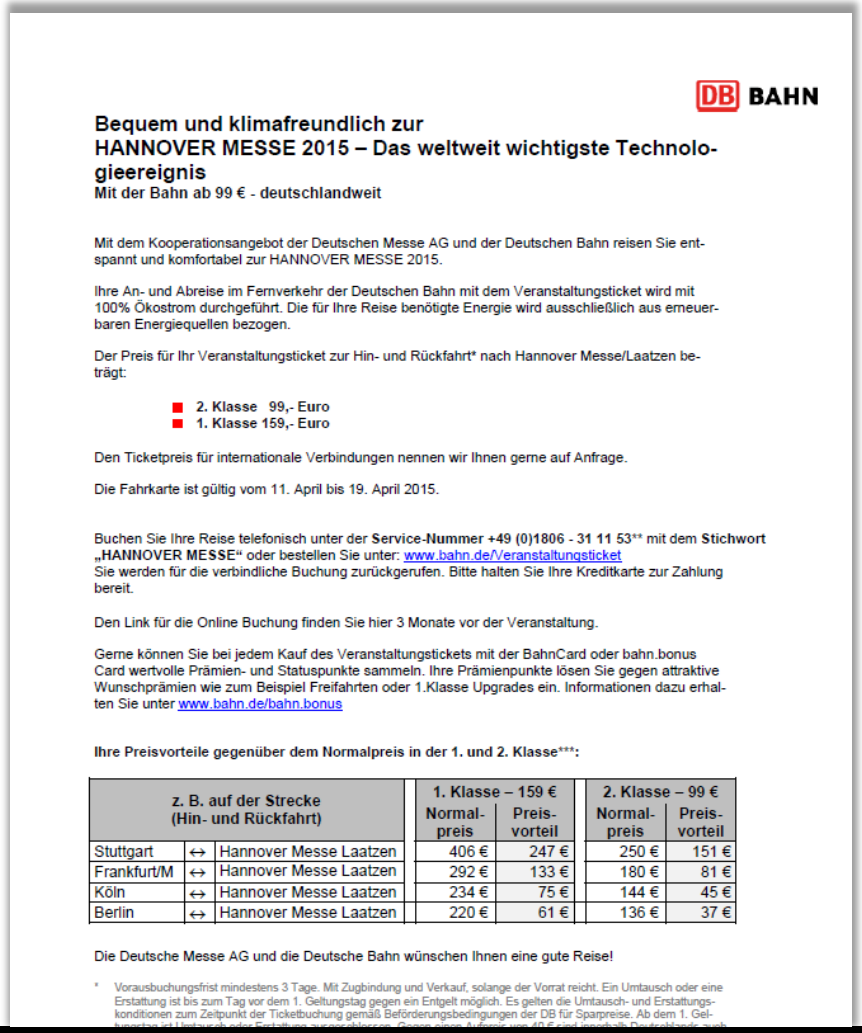
Buchen Sie Ihre Reise telefonisch unter der **Service-Nummer +49 (0)1806 - 31 11 53**** mit dem **Stichwort „HANNOVER MESSE“** oder bestellen Sie unter: www.bahn.de/Veranstaltungsticket
Sie werden für die verbindliche Buchung zurückgerufen. Bitte halten Sie Ihre Kreditkarte zur Zahlung bereit.

Den Link für die Online Buchung finden Sie hier 3 Monate vor der Veranstaltung.

Gerne können Sie bei jedem Kauf des Veranstaltungstickets mit der BahnCard oder bahn.bonus Card wertvolle Prämien- und Statuspunkte sammeln. Ihre Prämienpunkte lösen Sie gegen attraktive Wunschprämien wie zum Beispiel Freifahrten oder 1.Klasse Upgrades ein. Informationen dazu erhalten Sie unter www.bahn.de/bahn.bonus

Quelle: hannovermesse.de

Phishing | fiktives Szenario



DB BAHN

Bequem und klimafreundlich zur HANNOVER MESSE 2015 – Das weltweit wichtigste Technologiereignis
Mit der Bahn ab 99 € - deutschlandweit

Mit dem Kooperationsangebot der Deutschen Messe AG und der Deutschen Bahn reisen Sie entspannt und komfortabel zur HANNOVER MESSE 2015.

Ihre An- und Abreise im Fernverkehr der Deutschen Bahn mit dem Veranstaltungsticket wird mit 100% Ökostrom durchgeführt. Die für Ihre Reise benötigte Energie wird ausschließlich aus erneuerbaren Energiequellen bezogen.

Der Preis für Ihr Veranstaltungsticket zur Hin- und Rückfahrt* nach Hannover Messe/Laatzen beträgt:

- **2. Klasse 99,- Euro**
- **1. Klasse 159,- Euro**

Den Ticketpreis für internationale Verbindungen nennen wir Ihnen gerne auf Anfrage.

Die Fahrkarte ist gültig vom 11. April bis 19. April 2015.

Buchen Sie Ihre Reise telefonisch unter der **Service-Nummer +49 (0)1806 - 31 11 53**** mit dem **Stichwort „HANNOVER MESSE“** oder bestellen Sie unter: www.bahn.de/Veranstaltungsticket
Sie werden für die verbindliche Buchung zurückgerufen. Bitte halten Sie Ihre Kreditkarte zur Zahlung bereit.

Den Link für die Online Buchung finden Sie hier 3 Monate vor der Veranstaltung.

Gerne können Sie bei jedem Kauf des Veranstaltungstickets mit der BahnCard oder bahn.bonus Card wertvolle Prämien- und Statuspunkte sammeln. Ihre Prämienpunkte lösen Sie gegen attraktive Wunschprämien wie zum Beispiel Freifahrten oder 1.Klasse Upgrades ein. Informationen dazu erhalten Sie unter www.bahn.de/bahn.bonus

Ihre Preisvorteile gegenüber dem Normalpreis in der 1. und 2. Klasse*:**

z. B. auf der Strecke (Hin- und Rückfahrt)			1. Klasse – 159 € Normalpreis	1. Klasse – 159 € Preisvorteil	2. Klasse – 99 € Normalpreis	2. Klasse – 99 € Preisvorteil
Stuttgart	↔	Hannover Messe Laatzen	406 €	247 €	250 €	151 €
Frankfurt/M	↔	Hannover Messe Laatzen	292 €	133 €	180 €	81 €
Köln	↔	Hannover Messe Laatzen	234 €	75 €	144 €	45 €
Berlin	↔	Hannover Messe Laatzen	220 €	61 €	136 €	37 €

Die Deutsche Messe AG und die Deutsche Bahn wünschen Ihnen eine gute Reise!

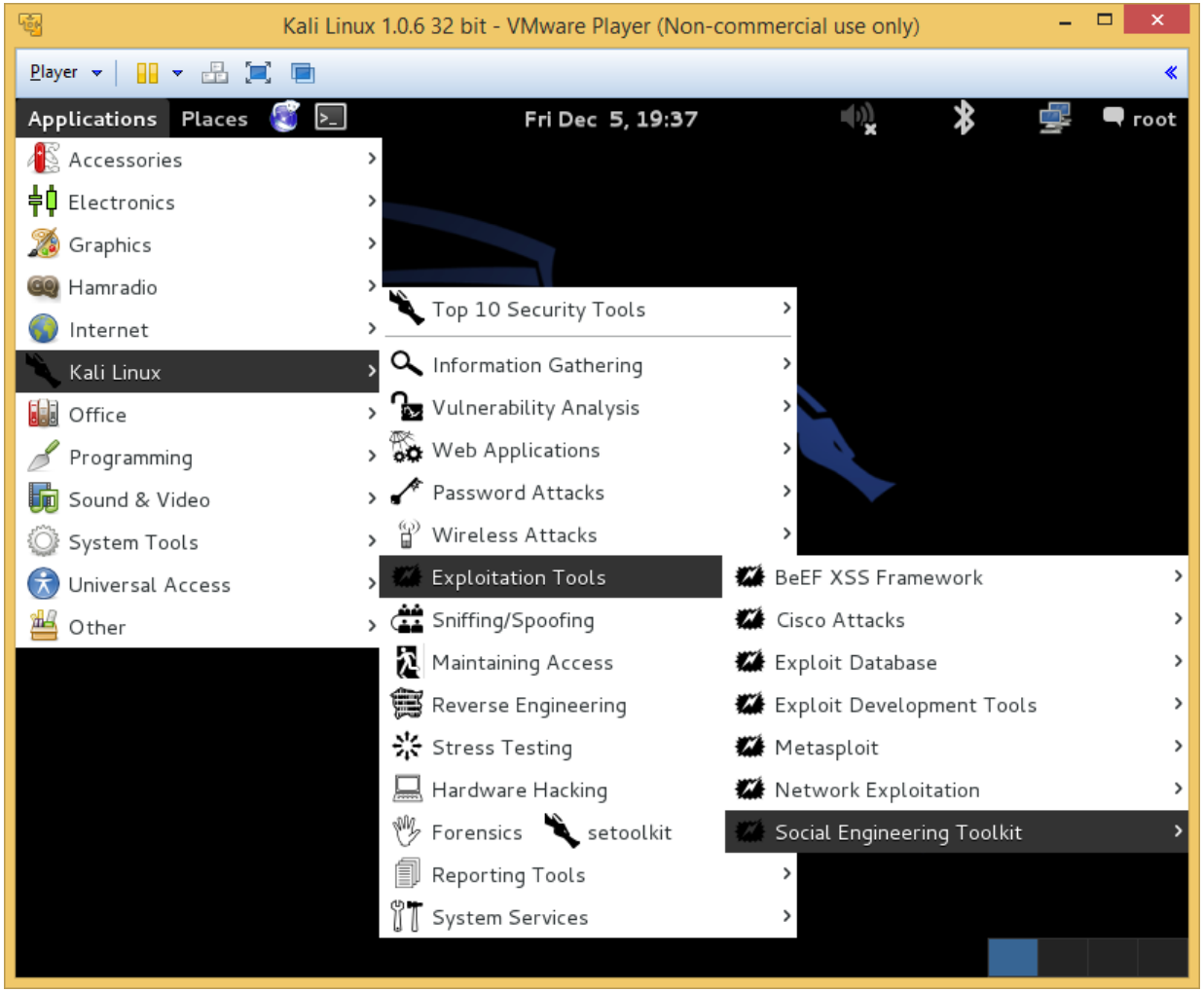
* Vorausbuchungsfrist mindestens 3 Tage. Mit Zugbindung und Verkauf, solange der Vorrat reicht. Ein Umtausch oder eine Erstattung ist bis zum Tag vor dem 1. Geltungstag gegen ein Entgelt möglich. Es gelten die Umtausch- und Erstattungskonditionen zum Zeitpunkt der Ticketbuchung gemäß Beförderungsbedingungen der DB für Sparpreise. Ab dem 1. Gel-

- 1. Leicht zu fälschen
  - » Anderes Layout, da Sonderaktion
  - » Telefon oder Online
- 2. Vertrauensvolle Namen
  - » Hannover Messe & Deutsche Bahn
- 3. Lukratives Angebot
  - » Es kann viel Geld gespart werden
- 4. Strategischer Verteiler
  - » An alle Firmen des vorherigen Jahres
  - » Auffordern zum Verteilen an Kunden

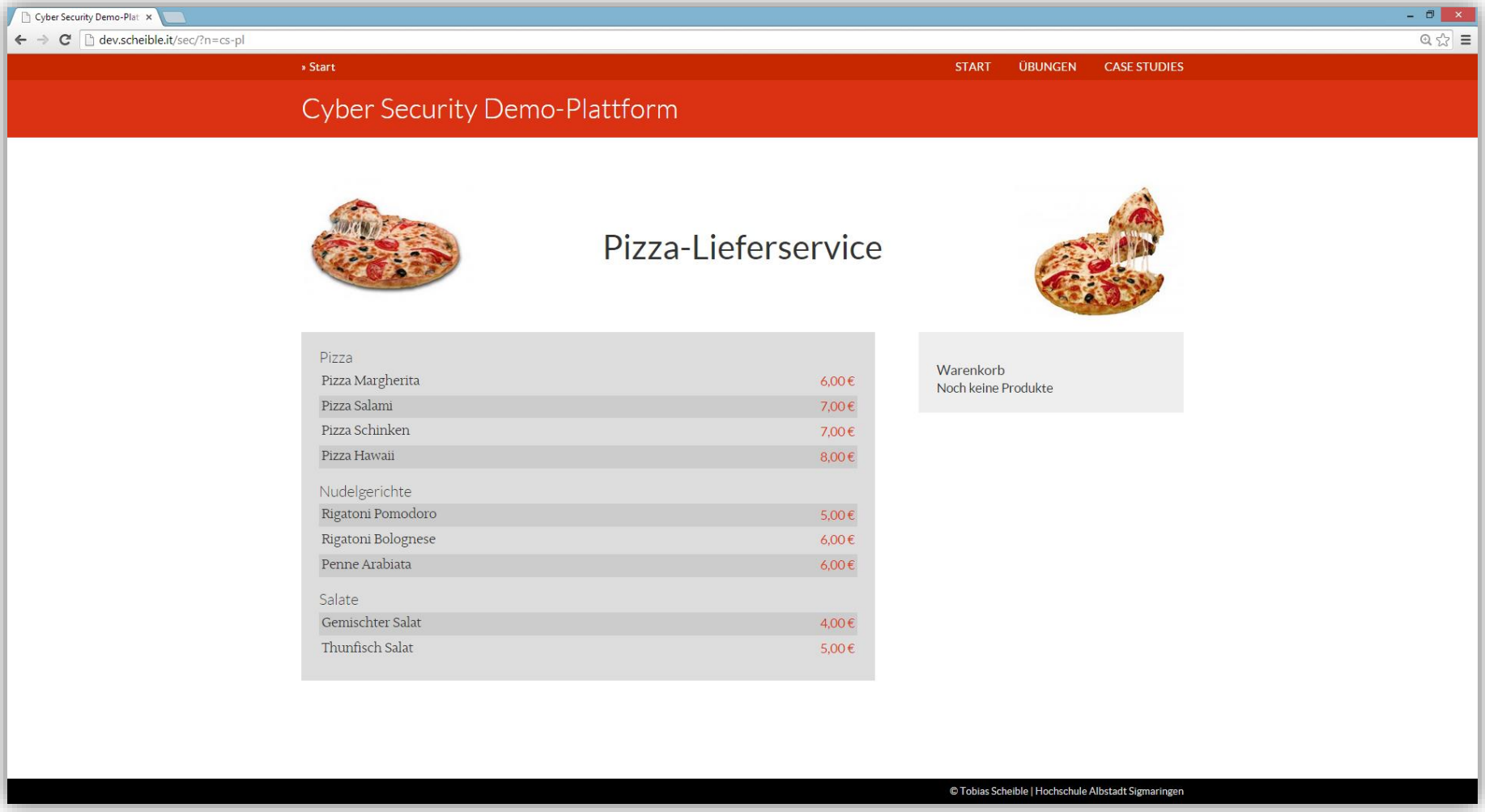
Websites manipulieren

- Phising-Seiten
  - » Phising-Seiten können sehr einfach mit Generatoren erstellt werden
  - » Zum Teil fällt ein falscher Login nicht einmal auf
  - » Beispiel: Eigene Phising-Seiten erstellen

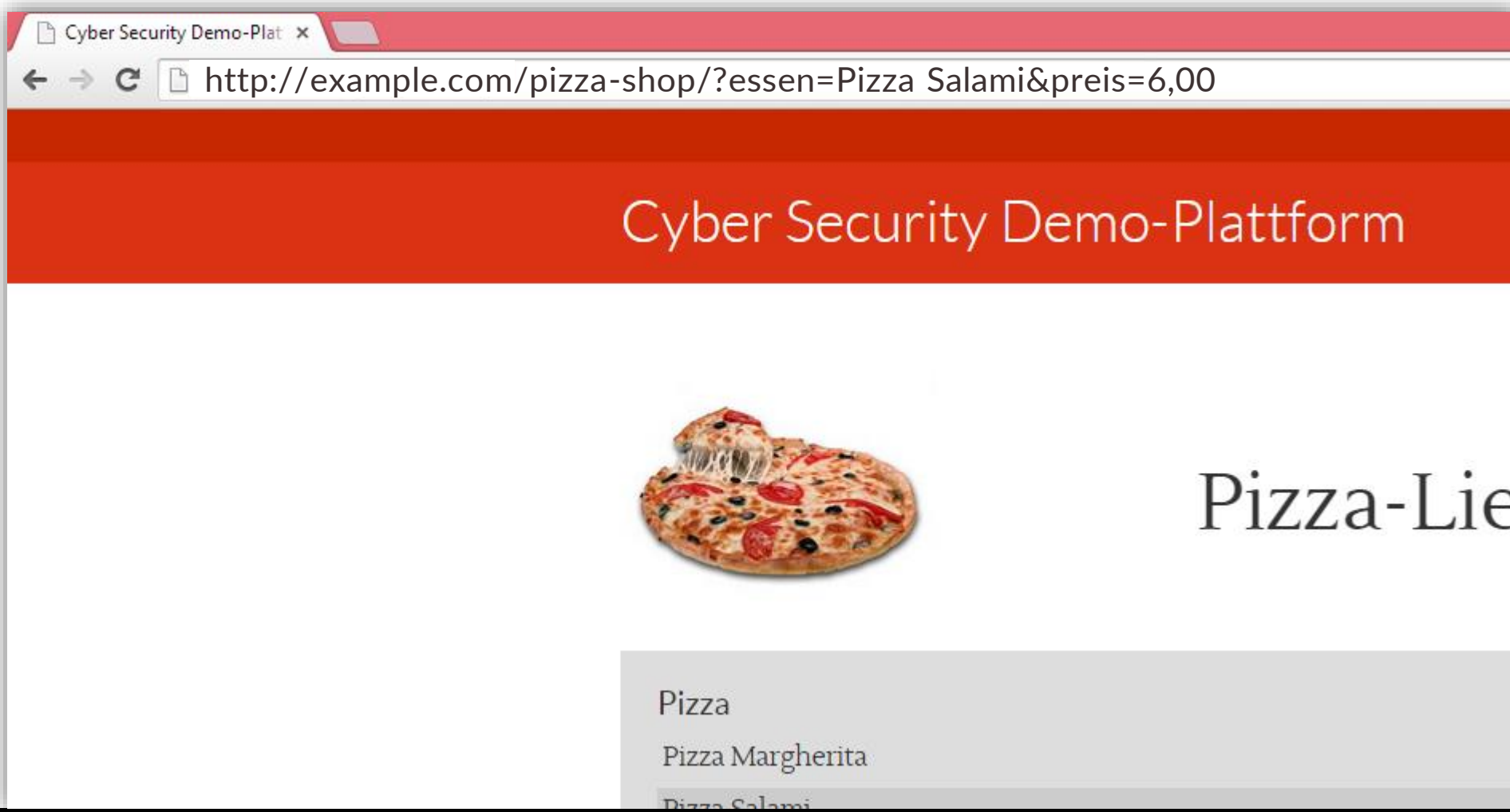
Websites manipulieren



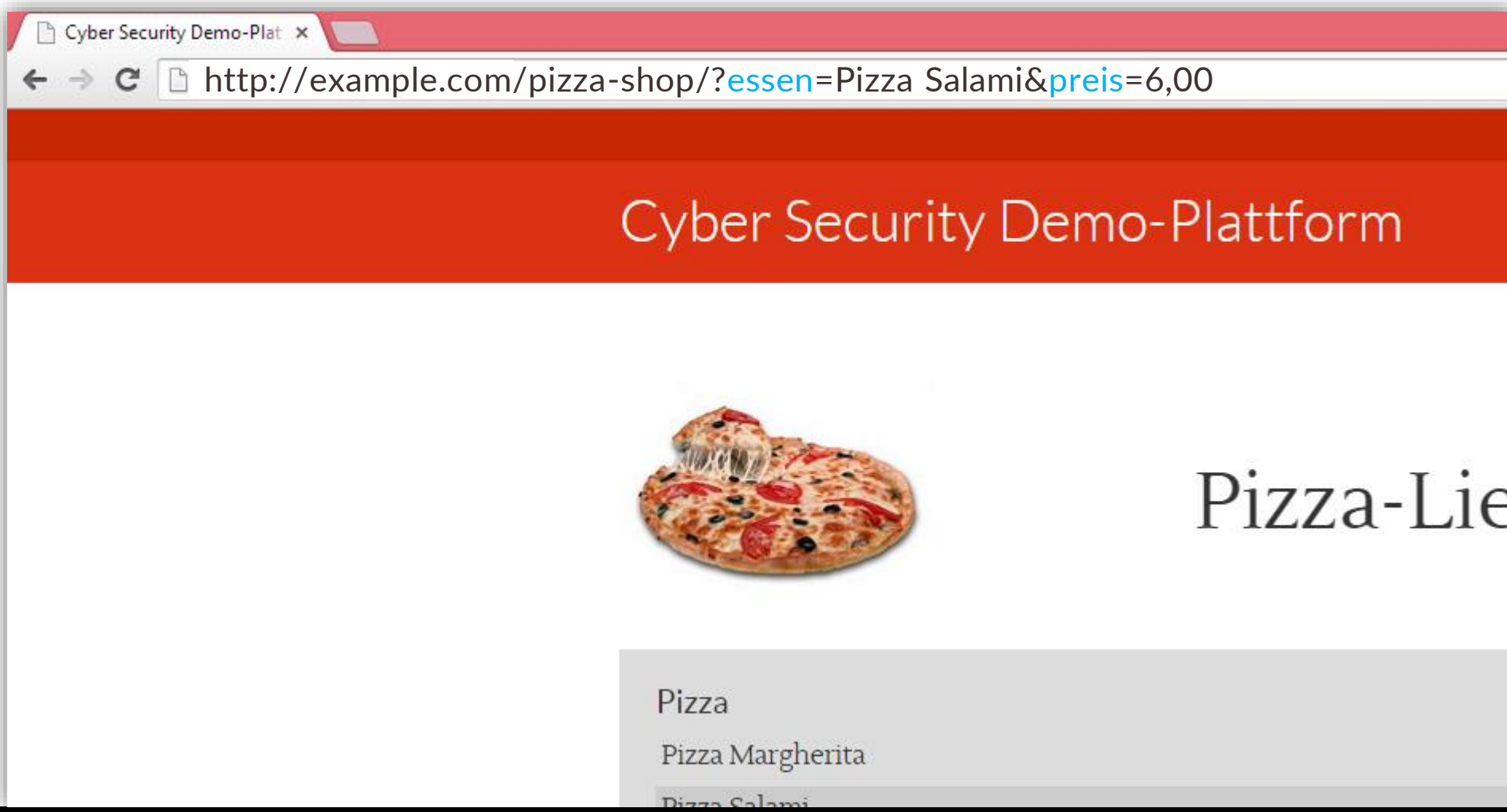
Google Hacks #2



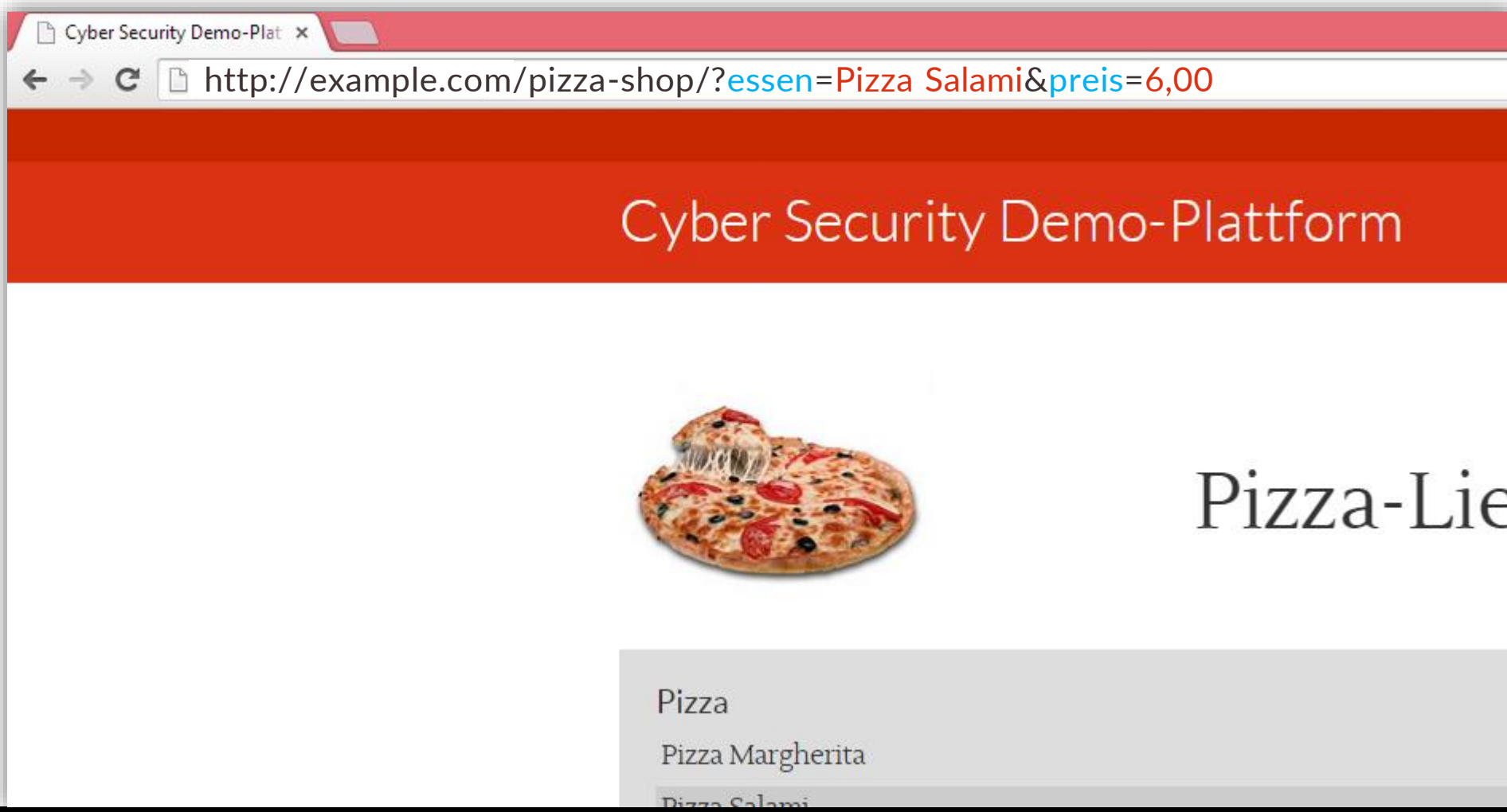
Google Hacks #2



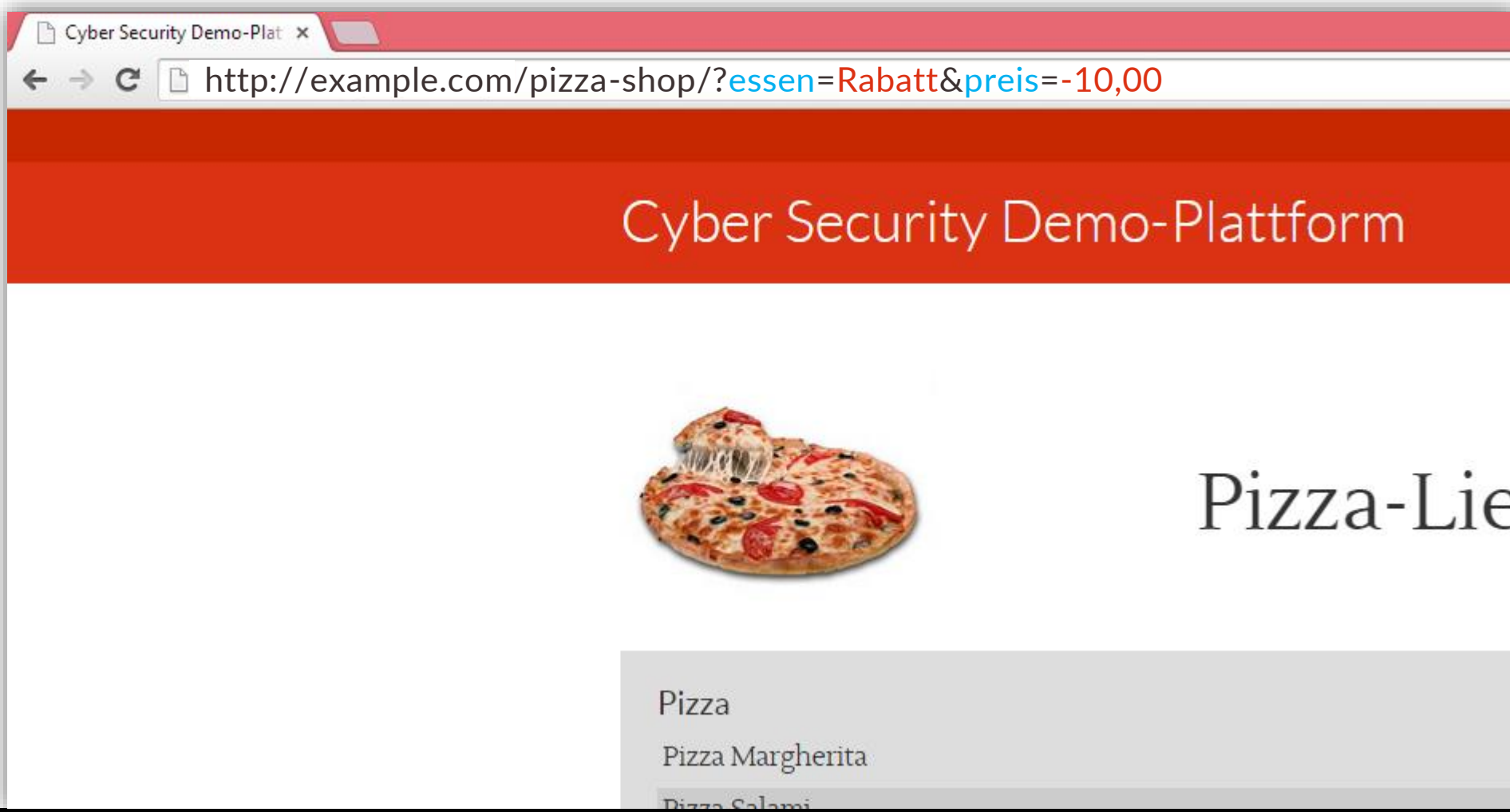
Google Hacks #2



Google Hacks #2



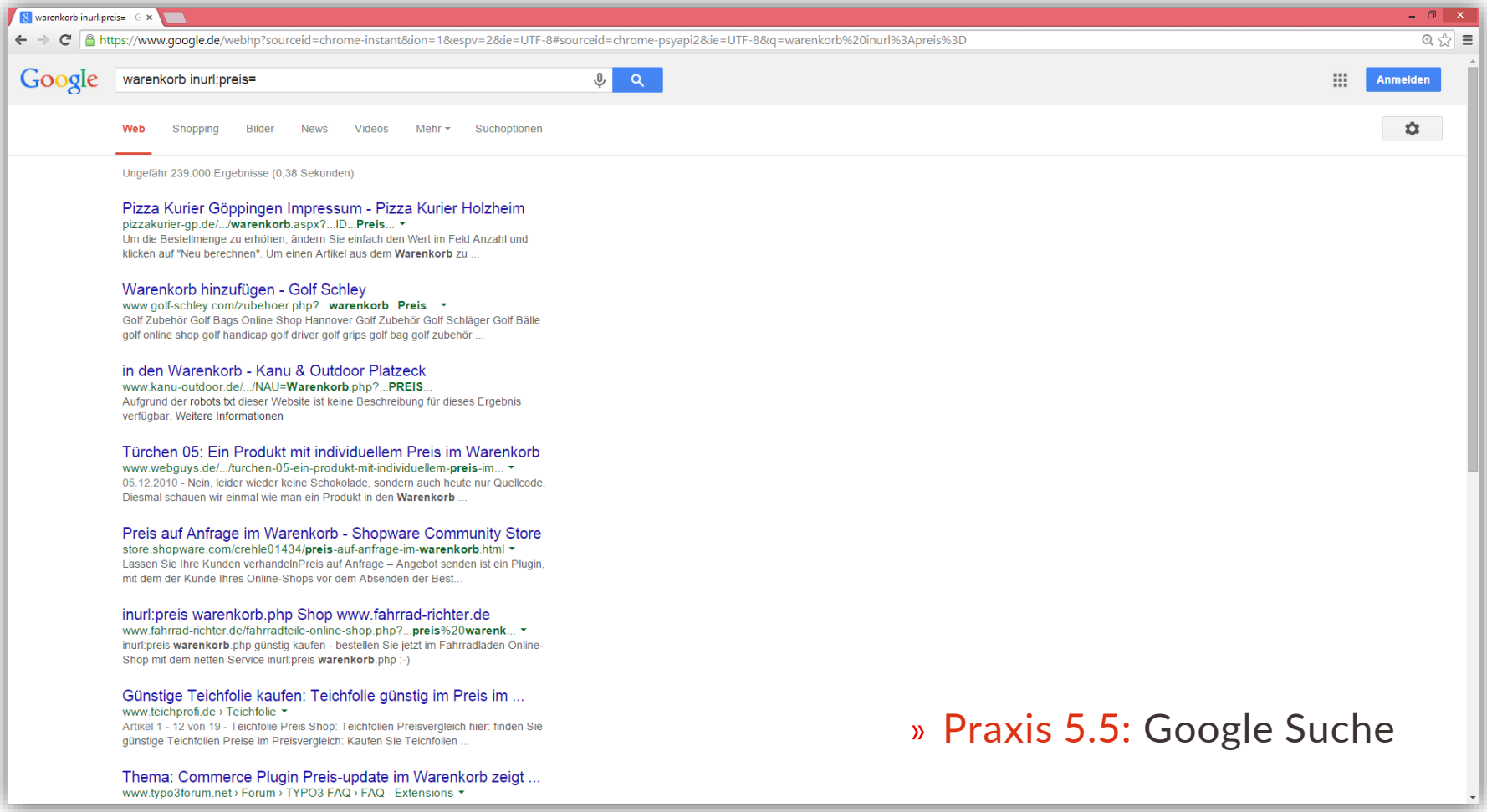
Google Hacks #2



Google Hacks #2

Google Hacks #2

Google Hacks #2



» Praxis 5.5: Google Suche

6. Cyber Defense

Workshop Agenda

- 1. Cyber Security
- 2. System Security
- 3. Network Security
- 4. Data Security
- 5. Web Security
- 6. Cyber Defense
  - » Verteidigungsmaßnahmen
  - » Best Practice

Verteidigungsmaßnahmen

- 1. Sicheres Passwort wählen
  - » Einfache Passwörter können schnell geknackt werden
  - » Bekannte Passwörter werden als erstes durchprobiert
  - » Komplizierte Passwörter verfehlen ihren Zweck
  - » z.B. Passwortkarte verwenden (Quelle: c‘t)

„‘123456‘ ist eines der häufigsten Passwörter, aber noch lange kein schlechtes!“

Heise News

Verteidigungsmaßnahmen

- 2. Neueste Updates installieren
  - » Mit Veröffentlichung der Updates werden auch die Sicherheitslücken publik
  - » Durch veraltete Software wird man zur Zielscheibe von Angreifern
  - » z.B. automatische Updates verwenden

„60 Prozent aller Angriffe erfolgen über bereits geschlossene Sicherheitslücken.“

Microsoft, CeBit 2013

Verteidigungsmaßnahmen

- 3. Spezielle Software nutzen
  - » Bei weit verbreiteter Software sind auch mehr Schwachstellen im Umlauf
  - » Angriffe auf seltene Software sind schwieriger
  - » z.B. Browser online-Banking

„Wer sich weiter absichern möchte, vermeidet Bankgeschäfte mittels Browser und nutzt statt dessen dedizierte Banking-Software.“

Heise News

Verteidigungsmaßnahmen

- 4. Sicherheits-Software verwenden
  - » Zusätzliche Hürde für Angreifer
  - » Inhalte werden untersucht, bevor sie geöffnet werden
  - » z.B. Avira Viren-Scanner installieren

„Überprüfen Sie Ihren Computer auf Befall. Nutzen Sie einen Virenscanner.“

Polizeidirektion Hannover

Verteidigungsmaßnahmen

- 5. Restriktive Konfigurationen
  - » Nur die notwendigsten Berechtigungen zulassen
  - » Angriffsfläche verringern bzw. möglichst klein halten
  - » z.B. Flash-Plugin in Firefox nur mit Zustimmung ausführen

„Die wichtigste Sicherheitsfunktion ist, dass die im Rechner verbauten Festplatten (SATA, PATA) von c't Bankix aus unerreichbar sind.“

Heise News

Verteidigungsmaßnahmen

- 6. Gesunde Skepsis
  - » E-Mails und Daten von Fremden gegenüber skeptisch sein
  - » Nicht unter Druck setzen lassen und lieber noch einmal nachfragen
  - » z.B. Bankdatenaktualisierung telefonisch hinterfragen

„Die Methode des ‚Social Engineerings' verspricht in Firmen mit starken IT-Sicherheitsvorkehrungen große Erfolge für den Angreifer."

BMWi Infobroschüre

Best Practice

- System und Programme schlank und aktuell halten
- Möglichst konservative Rechtevergabe und Konfigurationen
- Verschiedene Systeme verwenden
- Lieber noch einmal auf alternativem Weg nachfragen
- Mit Fehlinformationen gezielt Fallen stellen
  - » Beispiel: Versteckte Felder auf Web-Logins
  - » Notebook mit Gastbenutzer und Überwachungssoftware
  - » Smartphone reagiert auf falsche Pin Eingabe
  - » Austausch von Black Lists und Angreifer Daten


Fragerunde

Vielen Dank!

Präsentation bald auf der Website:
http://cyber-security-workshop.de