Ing. Joseph M. Riedinger

FH Wiener Neustadt	*- Lektor*
Akademie f. Recht u. Steuern	*- Vortragender*
Cybercrime Unit LKA NÖ	*- Leiter*
Cogito-IT Datacenter Systemhaus GmbH	*- Founder & Owner*

Outstanding Opportunities in Informationtechnology

Was wir in dieser kurzen Zeit versuchen werden…

- Einfluss und Auswirkung des Internet
  - Wir fragen die Wissenschaft….
- Wie gehen wir mit unseren Daten um?
  - Die Sache mit den Häkchen….
- Was bitte ist IoT?
  - Wenn der Kühlschrank mit dem Lieferanten….
- Mein Auto ist im Internet?
  - Datenkrake Auto
- Autodiebstahl 4.0
  - Car Hack & Keyless Go
- Einbruch 2.0
  - Brechen wir doch in ein Haus ein…
- Maintarget Unternehmen
  - Ransomware, CEO-Fraud & DDoS-Erpressung
- Bitcoins & Blockchains
  - Wie und warum funktioniert das?
- Darknet
  - „Show me the way to the next…..“

0664-132-97-97

Lektor Fachhochschule Wiener Neustadt
"WIRTSCHAFTSKRIMINALITÄT & CYBER CRIME"

- Kooperation FH WN – BM.I – BM.F
- greift brandaktuelle Themen in der Kriminalitätsbekämpfung auf
- bereitet die TeilnehmerInnen auf die Bekämpfung von Wirtschaftskriminalität und Cyber Crime vor.
- Bekämpfung der Erscheinungsformen
- Ganzheitliches Wissen aus den Themengebieten Recht, Wirtschaft, IT und Ermittlung

- *Wissensvermittlung sowohl für öffentl. Bedienstete als auch für Personen aus Wirtschaft und Privatleben*

FACHHOCHSCHULE
WIENER NEUSTADT
Austrian Network for Higher Education

0664-132-97-97

Vortragender Akademie f. Recht u. Steuern
„DIGITALE FORENSIK & CYBER CRIME"

- Datenschutz
- Disaster Recovery
- Forensische Analyse
- IT-Sicherheit
- IT-Recht (*z.B. Datenschutzgrundverordnung der EU*)

Weiterbildung für Rechtsanwälte und Steuerberater im Bereich Recht und IT

ARS
AKADEMIE FÜR RECHT, STEUERN & WIRTSCHAFT

0664-132-97-97

Owner & Founder

COGITO-IT DATACENTER SYSTEMHAUS GMBH

- Erstellung und Umsetzung von Sicherheitskonzepten
  (Ransomware-Schutz, Intrusion prevention/detection etc.)
- Entwicklung von Webdatenbanken/anwendungen
  (auf Basis SQL-Server/.NET)
- Systemwiederherstellung
  (nach Datenverlust/Verfügbarkeitssperre etc.)
- Virtualisierung
- Optimierung
- Replikation
- Off-Site Sicherung

COGITO
outstanding opportunITies ...

- *Betreuung hochsensibler Kunden im Bereich Netzwerk und Security*

0664-132-97-97

Owner & Founder
COGITO-IT DATACENTER SYSTEMHAUS GMBH

Referenzen

Deutsche Lufthansa AG
Austrian Airlines AG
SWISS International Airlines
….
Rechtsanwalt Dr. J. Stieldorf
Rechtsanwalt Dr. Christoph Kopetzky
Rechtsanwältin Dr. Kordula Fleiß-Goll
Steuerberatungskanzlei Mag. Christian Zeidler
….
National Security Austria
Sicherheitsunternehmen für Botschaften
….
Industriebetriebe
KMUs
Verlage
….

COGITO
outstanding opportunITies ...

0664-132-97-97

Dienstleistung Datenschutzbeauftragter

Owner & Founder
COGITO-IT DATACENTER SYSTEMHAUS GMBH

Datenschutzbeauftragter

Werden in einem Unternehmen personenbezogene oder sensible Daten dergestalt verarbeitet, dass die Art oder der Umfang dieser Verarbeitung eine umfangreiche regelmäßige und systematische Überwachung erforderlich macht, **muss** dieses Unternehmen ex lege einen Datenschutzbeauftragten benennen.

www.cyberprotection.at
www.cyberadvocat.at

0664-132-97-97

Leiter Cybercrime Unit LKA NÖ

„DIGITALE FORENSIK & CYBER CRIME"

- Ermittlungen im Internet
- Sicherstellung von Datenträgern jeder Art
- Forensische Analyse von Datenträgern im Verfahren
- Live-Forensik
- Kfz-Forensik

POLIZEI

- *Ermittlungen für Gerichte und Staatsanwaltschaften*
- *Forensische Sicherung und Auswertungen in Gerichtsverfahren*
- *Bekämpfung von Cybercrime*

CYBER CRIME

Ist das Internet der neue Wilde Westen?

Informationen und Hilfestellungen
für junge und "jüngere"
Internetuser

Das Internet?

„Das Internet ist die erste Erfindung der Menschheit, die sie selbst nicht mehr versteht. Das größte anarchistische Experiment, das es jemals gab."

(Eric Schmidt, US-amerikanischer Informatiker und Manager und war von April 2011 bis zum 10. August 2015 Executive Chairman von Google)

0664-132-97-97

Wie gehen wir mit unseren privaten Daten um?

Die Sache mit den Häckchen….


Das neue I-Phone Erkennt deinen Finger.
Sie werden 600 Euro bezahlen...
Um uns ihre Fingerabdrücke zu - geben!
PRISM PROJECT
NSA
CIA

0664-132-97-97

Quelle: ADAC

Datenkrake Auto

Das Wichtigste in Kürze:

Der ADAC hat **vier Auto-Modelle** darauf untersucht, welche Daten gespeichert und gesendet werden.

Einen Mercedes der B-Klasse mit dem System «me-connect», einen Renault Zoé sowie zwei Modelle von BMW, den 320 und das Elektromobil i3.

Die Autos senden beispielsweise **Telefonkontakte**, Sitzpositionen oder abgespielte Musiktitel an die Hersteller.

Verschiedene Automobilclubs fordern mehr Transparenz bezüglich dieser Datenverarbeitung.

Hersteller müssten eine **Ausschalt-Funktion** bieten!

0664-132-97-97

Quelle: ADAC

Datenkrake Auto

Hersteller-Zugriff aus der Ferne

Brisant:

Autohersteller können auch auf das einzelne Auto aus der Ferne zugreifen. Renault kann beispielsweise beim Elektromobil Zoé das Aufladen der Antriebsbatterie verhindern.

Der Fahrzeughersteller kann sogar den Antriebs-Akku abschalten. Und zwar dann, wenn der Verbraucher beispielsweise die Leasinggebühr für den Akku nicht bezahlt hat.
So kann Renault verhindern, dass das Auto wieder aufgeladen werden kann.

0664-132-97-97

Quelle: ADAC

Datenkrake Auto

Auszug der erhobenen Daten der Fahrzeuge:

BMW i3

Mittels Last State Call (automatisch nach dem Ausschalten der Zündung und Abschließen des Autos)

- Detaillierte Daten der Antriebsbatterie (wie Ladezustand, Zelltemperatur usw.)
- Gewählter Fahrmodus (eco, eco plus, sport)
- Einsatzdaten des Range Extenders (REX)
- Wie oft wurde der Ladestecker eingesteckt?
- Wie und wo wurde geladen, wie stark war die Antriebsbatterie entladen?
- Kilometerstand bei Bedienvorgängen wie z.B. Laden.
- GeoPosition der 16 zuvor benutzten Ladestationen
- Rund 100 letzte Abstellpositionen des Fahrzeugs.

Quelle: Spiegel online

Chrysler – Car – Hack

Charlie Miller und Chris Varasek

Sicherheitslücke im Uconnect
- Internetanbindung Chrysler-Fahrzeuge
- Entertainment- und Navigationsfunktionen,
- ermöglicht Anrufe
- bietet WLAN-Hotspot an

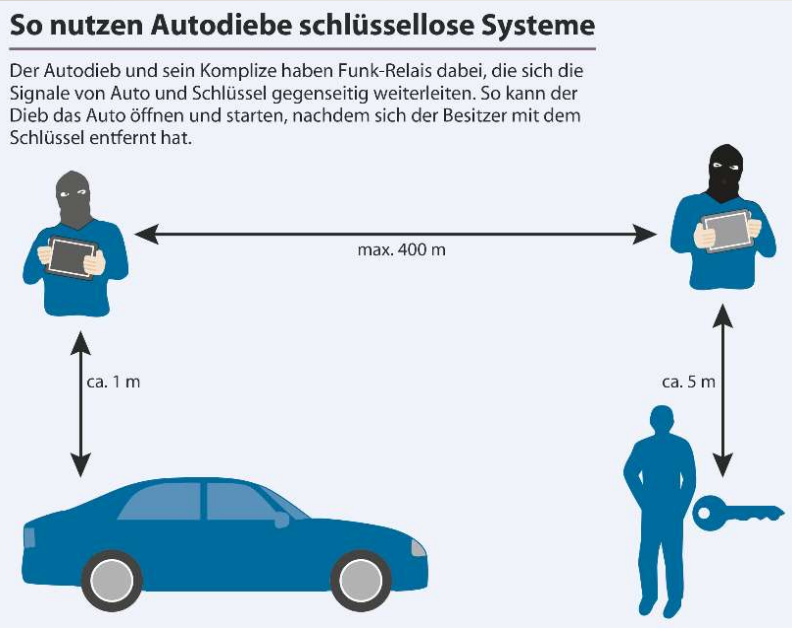
  - stellten Lüfter an,
  - schickten ein Bild von sich auf den Multimedia-Bildschirm
  - drehten Musik laut. (Drehen am Lautstärkeregler ohne Wirkung)
  - Stoppen des Motors des Jeeps, deaktivieren der Bremsen etc. per Tastenklick

Angriffszenario KeylessGo

KeylessGo-Systeme:	schlüsselloser Zugang Öffnen, Verriegeln und Starten
Fahrzeugschlüssel:	nicht mehr in die Hand zu nehmen. enthält alle Funktionen für Zutritt und Fahrberechtigung
Fahrzeug:	erkennt über Sensoren bzw. Induktionsantennen in Stoßstangen, Tankverkleidung und Türen die Annäherung
Starten und Abstellen:	im Innenraum über eine Start/Stopp-Taste. Beim Verlassen des Fahrzeuges erfolgt Verriegelung automatisch.

0664-132-97-97

Angriffszenario KeylessGo



0664-132-97-97

Statistik?

Internet-Sicherheitsbericht 2018 -Cybercrime

- eine Million Opfer von Cyber-Attacken pro Tag.
- Schaden pro Nutzer statistisch 288 EUR pro Jahr
- Schaden 6,47 Milliarden Euro/weltweit 208 Milliarden US Dollar (lukrativer als Drogenhandel!)
- 67% der Erwachsenen schon einmal Opfer von Cyberkriminalität
- Kaspersky Lab 2015 (sic!) : 53% der weltweiten Rechner in Unternehmensnetzwerken mindestens eine Malwareattacke
- Gegen Firmenrechner werden dreimal häufiger zu Office-Anwendungen eingesetzt, als bei Angriffen auf private Computer.

Quelle: nic.at und Computer Emergency Response Team (CERT.at)

Statistik?

durchschnittliche Dauer bis zur Entdeckung von Schadsoftware auf IT-Systemen:

- 2011: 416 Tage
- 2014 205 Tage
- 2015: 146 Tage
- 2016: 93 Tage
- 2018: 9 Tage

- Compliance Regeln zu wenig
- weitgehenden Schutz bietet nur zentrales Monitoring durch Security Operation Center

notwendig: weniger als 10 Minuten

QuelleFH Hagenberg

Statistik?

Eines von 5 Kindern erhalten sexuell motivierte Kontaktversuche über das Internet.

Der sogenannte Identitätsdiebstahl nahm im Zeitraum 2010 bis 2012 weltweit um mehr als 1300 % zu!

Regierungen bilden bereits offensive und defensive Cyber War Departments weltweit

0664-132-97-97

Computerkriminalität

Computer werden zur Begehung strafbarer Handlungen benützt

- Internetbetrug
- Identitätsdiebstahl
- Spaming
- Phishing
- Kinderpornografie
- Urheberrechtsverletzung
- Mobbing
- usw….

Computerkriminalität

Computer als Ziel strafbarer Handlungen

Versenden von Viren und Würmern

Industriespionage

Softwarepiraterie

Hacking

Ransomware

verschlüsselt Dateien

- auf der lokalen Festplatte
- auf sämtlichen erreichbaren, für den jeweiligen Nutzer berechtigten Netzwerklaufwerke
- auf verbundenen Backuplaufwerken

Ransomware

- Täter übermitteln ein Werkzeug zur Wiederherstellung der Dateien.
- tatsächlicher Schaden kann nur geschätzt werden,
- Viele Betroffene bringen den Fall nicht zur Anzeige.

Ransomware


CryptoLocker
Your personal files are encrypted!
Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet; the server will destroy the key after a time specified in this window. After that, nobody and never will be able to restore files...
To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.
Click «Next» to select the method of payment and the currency.
Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.
Private key will be destroyed on
20/10/2013
11:11
Time left
71 : 52 : 49

Was ist die Blockchain?

Am Anfang jeder Blockchain steht ein Netzwerk von Nutzern (Nodes), die untereinander verbunden sind (ein Peer-to-Peer-Netzwerk) und in irgendeiner Form Geschäfte abzuwickeln haben, die auf Vertrauen basieren. (Finanztransaktionen, Versicherung, Umwidmung eines Grundstücks etc.) Üblicherweise wird für ein solches Geschäft ein Mittelsmann eingeschaltet, eine sogenannte „trusted third party“. (z.B. Banken, bei denen Zahler und Empfänger ihre Konten haben, Kreditkartenanbieter etc.)

Was ist die Blockchain?

Eine Blockchain ist eigentlich nur eine Textdatei und nicht mehr als eine Art virtuelles Hauptbuch (Buchungsjournal), in das alle Transaktionen, die jemals mit Bitcoins abgeschlossen wurden, eingetragen werden - und zwar von den Nutzern des Bitcoin-Systems selbst.

„Vorteile“ der Bitcoins?

Weltweit

Anonym

Keine Währungskonvertierungsverluste

Keine zentrale Knoten (Banken etc.)

Steuerfrei !

Vom „hash“ zur „block chain“

Für jede Transaktion wird ein Hashwert errechnet. Dabei wird den Daten der Transaktion durch eine Hashfunktion eine Zeichenfolge mit festgelegter Länge zugeordnet. Damit lässt sich eine größere Datenmenge, durch eine kleinere – den Hashwert – zusammenfassen. Da es sich um eine mathematische Funktion handelt, bleibt aber immer nachvollziehbar, welcher Datensatz sich hinter dem Hashwert verbirgt.

Vom „hash“ zur „block chain“

Mehrere dieser Transaktionen werden zu einem Block zusammengesetzt. Jeder Block kann seinerseits durch eine bestimmte Zeichenfolge identifiziert werden. In dieser Zeichenfolge, dem sogenannten „block header“ ist auch ein Hashwert enthalten. Dieser Hashwert ergibt sich aus der Zusammenfassung der Hashwerte aller Transaktionen des Blocks.

Warum ist das so sicher?

In diesem System können einzelne Transaktionen nun nicht verändert werden, ohne die gesamte Kette zu verändern. Denn bei einer Änderung der Transaktionsdaten ändert sich auch ihr Hashwert und damit zugleich der Hashwert im „block header“ des jeweiligen Blocks und in weiterer Folge auch alle nachfolgenden Blöcke. Jede neue Transaktion trägt also die Summe aller früheren Transaktionen in sich.

CEO - Fraud

Banküberweisung

Die Angreifer forschen aus, wer in der Lohnabteilung oder dem Finanzbereich des Unternehmens arbeitet.

Sie erstellen dann eine E-Mail, die vorgibt, z.B. vom Leiter der Abteilung zu stammen, und berichtet von einem Notfall, aufgrund dessen dringend Geld auf ein angegebenes Konto überwiesen werden muss…..

CEO - Fraud

Steuerbetrug

Cyberkriminelle versuchen Informationen über Sie und Ihre Kollegen zu stehlen, um in ihrem Namen Steuerbetrug begehen zu können. Sie forschen Ihre Organisation aus und finden heraus, wer Mitarbeiterdaten verarbeitet, wie z.B. die Personalabteilung.

Darauf aufbauend senden die Kriminellen E-Mails die vorgeben, von einem leitenden Angestellten oder jemandem aus der Rechtsabteilung zu stammen, und fordern bestimmte Dokumente mit personenbezogenen Inhalten an, die sofort bereitgestellt werden müssen.

CEO - Fraud

Anwalts-Nachahmung

Nicht alle CEO Fraud Angriffe bauen nur auf E-Mail, andere Methoden wie z.B. Anrufe, werden auch genutzt.

In diesem Szenario senden die Angreifer zunächst eine E-Mail, die scheinbar von einer Führungskraft stammt. Darin wird angekündigt, dass in Kürze ein Anwalt in einer dringenden Angelegenheit anrufen wird.

Ein Krimineller ruft dann tatsächlich an und gibt vor, der angekündigte Anwalt zu sein. Er erzeugt eine große Dringlichkeit und spricht über zeitkritische, sehr sensible Themen.

DDoS – Distributed Denial of Service

- Angriffe auf Online-Verfügbarkeit und der dahinterliegenden Systeme
- die Systeme des Opfers werden überlastet
- dadurch nur mehr eingeschränkt oder schlimmstenfalls gar nicht mehr verfügbar.
- In den letzten zwei Jahren starke Zunahme
- insbesondere diesbezügliche Erpressungen steigen

Generell bei Cyber-Erpressungen

- Lösegeld auf keinen Fall bezahlen.
- keinerlei Garantie, dass keine weiteren Angriffe folgen
- Wahrscheinlichkeit für Nachahmungs- und Wiederholungstäter steigt.
- CERT.at (www.cert.at)
- Meldestelle des Bundeskriminalamts zur Bekämpfung der Cyber-Kriminalität (against-cybercrime@bmi.gv.at).