RÜHLCONSULTING

Social Engineering: Hirngespinst paranoider Sicherheitsexperten oder reale Gefahr?

RÜHLCONSULTING

Ein paar **kurze** Worte zur Vorstellung…

RÜHLCONSULTING

Zum Unternehmen

Bild: Firmensitz im High-Tech-Center Nürnberg-Schafhof

- Spezialisierung: **Sicherheitsfragen im Mittelstand**
- Gegründet: 2008
- Geschäftsführender Gesellschafter: Uwe Rühl
- Geschäftssitz: Nürnberg

RÜHLCONSULTING

Unsere Tätigkeitsfelder

Audits	• Analysen, Bewertungen, Lieferantenaudits, interne Audits
Beratung	• Projektmanagement, Konzeption, Implementierung
Trainings	• Schulungen und Trainings, Sensibilisierungsmaßnahmen
Partner	• Externe spezialisierte Ressource, z.B. als ISMS-Beauftragter

RÜHLCONSULTING

Unsere Expertise

Informationssicherheitsmanagement

- DIN ISO/IEC 27001 „Native" und IT-Grundschutz

Business-Continuity-Management

- BS 25999-2 // ISO 22301
- IRBC nach ISO/IEC 27031 und ITIL

Risikomanagement

- ISO 31000 und ISO/IEC 27005

IT-Service-Management

- ITIL und ISO/IEC 20000-1

RÜHLCONSULTING

Zu meiner Person

Auditor, Berater und Trainer

- Berufener ISO 27001 Auditor
- Erfahrungen Informationssicherheit: seit 1997

Mein Herz schlägt für…

- … Informationssicherheit
- … Risikomanagement
- … Business-Continuity-Management

Beruflicher Weg

- Lehre zum Versicherungskaufmann
- Studium der Betriebswirtschaft an der VWA in Kassel
- Langjähriger IT Security Manager bei deutschen Versicherungskonzernen
- Bei der RÜHLCONSULTING seit 2011

RÜHLCONSULTING

Agenda

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe & wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Motivation und Ziele dieses Vortrags

RÜHLCONSULTING

Ziel ist es, eine Sensibilisierung für die Thematik zu erzeugen

Nur für das Problem sensibilisierte Personen können SE-Angriffe erkennen und effizient abwehren

Die Herausforderung für jeden Einzelnen besteht darin, reine Freundlichkeit und Hilfsbedürftigkeit von Angriffsversuchen zu unterscheiden

Ziel ist **nicht** die eigene „Ausbildung“ zum Social Engineer! ☺

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

„Social Engineering“ – Definitorisches

den Versuch, die menschliche Gesellschaft umzugestalten: *Social Engineering (Gesellschaftswissenschaft)*

eine (entwicklungs-)politische Tätigkeit, die aktiv soziale Gruppen schaffen und modulieren will: *Social Engineering (Politik)*

das gezielte Verwenden gestohlener Daten, um einer gutgläubigen Person weitere Daten wie z.B. Kennwörter oder Bankdaten zu entlocken: *Social Engineering (Sicherheit)*

[Quelle: Wikipedia, historisch]

Wie also lässt sich Social Engineering am Besten beschreiben?

Social Engineering ist **DIE KUNST DER TÄUSCHUNG**

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

„Social Engineering“ – Abgrenzung und Einteilung

Die Erpressung oder die direkte Bedrohung von Personen zählt nicht zum Bereich des Social Engineering

Ein Social Engineer hat immer das Ziel, seine Aktivitäten unbemerkt durchzuführen

Es wird unterschieden zwischen

- Computer-Based Social Engineering
- Human-Based Social Engineering
- Reverse Social Engineering

Ein Social Engineer hat grundlegende Fähigkeiten eines Profilers

Profiler – eine Definition

Ein Profiler (Profilersteller, Fallanalytiker) erstellt Täterprofile.
Die Tätigkeit bezeichnet man als operative Fallanalyse (profiling). Dabei erstellt der Profiler ein charakteristisches Erscheinungs- und Persönlichkeitsbild eines unbekannten Straftäters anhand von Indizien, Spuren am Tatort und den Umständen der Straftat. Die Begriffe Profiler und Profiling leiten sich von
(franz.) Profil= Umriss, Seitenansicht und von
(italien.) profilo, profilare = umreißen
ab.

[Quelle: Wikipedia, historisch]

Computer-Based Social Engineering

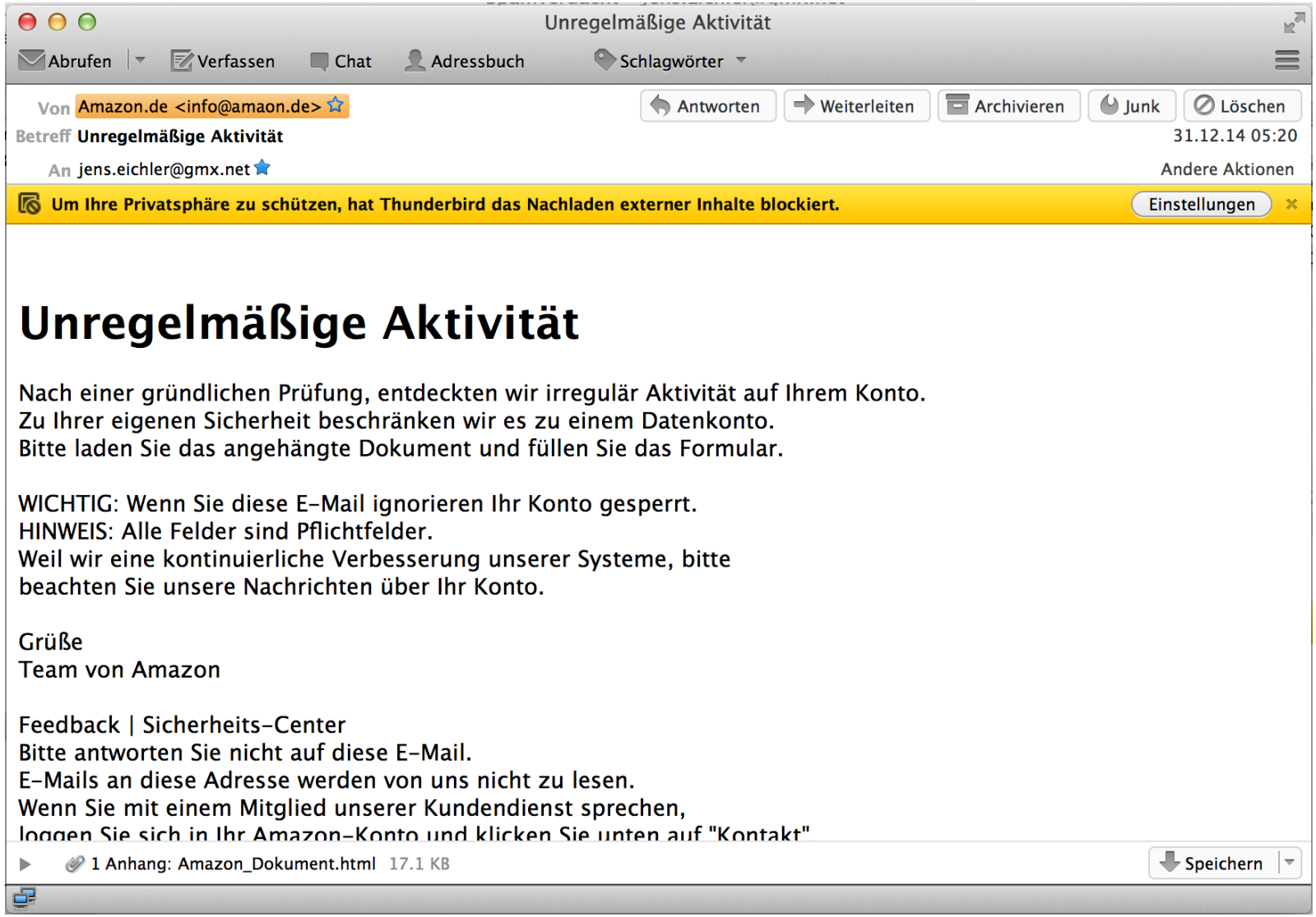
RÜHLCONSULTING

Beim „Computer-Based Social Engineering“ werden erforderliche Informationen mit technischen Hilfsmitteln beschafft.

Manipulierte Internetseiten, Mailanhänge oder Popup-Fenster mit Eingabefeldern sind nur einige Beispiele dafür.

Computer-Based Social Engineering

RÜHLCONSULTING



Computer-Based Social Engineering

RÜHLCONSULTING

Fwd: Wichtige PayPal Mitteilung

Von: Uwe Rühl

service@paypal.deschrieb:

PayPal

Sehr geehrte Kundin, Sehr geehrter Kunde,

seit dem 15.07.2014 ist das neue Zahlungssystem SEPA (Single Euro Payments Area) auch bei PayPal aktiv. Die Umstellung führt dazu, dass wir einige Kunden auffordern müssen sich zu verifizieren, damit unser System die Umstellung vollständig und ordnungsgemäß durchführen kann. Nach einer erfolgreichen Verifizierung wird die Umstellung automatisch durch unser System ausgeführt.

Die Verifizierung ist so schnell wie möglich durchzuführen, andernfalls wird Ihr Konto **(privat@uweruehl.de)** vorübergehend eingeschränkt.*

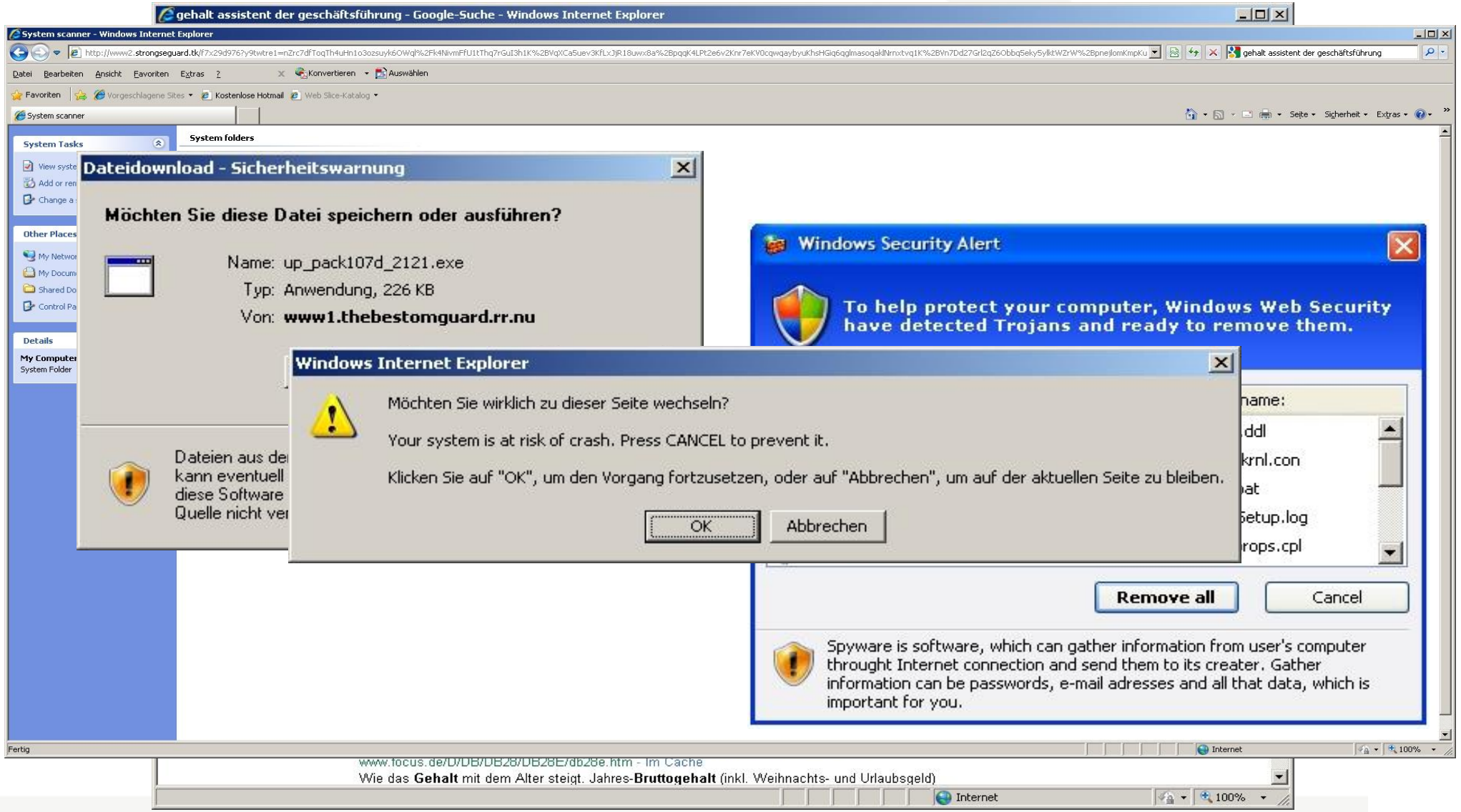
Vielen Dank für Ihr Verständnis.

Mit freundlichen Grüßen
Ihr Team von **PayPal.de**

Verifizierung jetzt durchführen

Computer-Based Social Engineering

RÜHLCONSULTING



Human-Based Social Engineering

Im Gegensatz zum Computer-Based Social Engineering werden beim „Human-Based Social Engineering“ die Informationen auf nicht-technischem Weg über die soziale Annäherung an Personen beschafft.

Reverse Social Engineering

Eine weitere Ausprägung des Social Engineering ist das Reverse Social Engineering. Ziel des Angreifers ist es hier, sich die gewünschten Informationen über das Opfer nicht selbst zu beschaffen, sondern einen Anwender dazu zu bringen, die Informationen freiwillig und aktiv an den Angreifer zu übermitteln.

Beispiel: Der Angreifer stellt sich telefonisch als neuer Supportmitarbeiter beim Opfer vor und hinterlässt für auftretende Probleme seine Rufnummer. Danach sorgt er für ein Problem und erreicht damit, dass das Opfer ihn kontaktiert anstatt den zuständigen Unternehmenssupport um Hilfe zu bitten.

- **Vorteil:** Beim „Reverse Social Engineering“ ist die Chance wesentlich geringer, dass die Opfer Verdacht schöpfen.
- **Nachteil:** Aufgrund einer langen und intensiven Vorbereitung ist „Reverse Social Engineering“ allerdings ein sehr aufwendiges Verfahren. Oftmals muss ein Zugang zum Netzwerk oder Rechner des Anwenders bestehen, um diese Methode anwenden zu können.

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

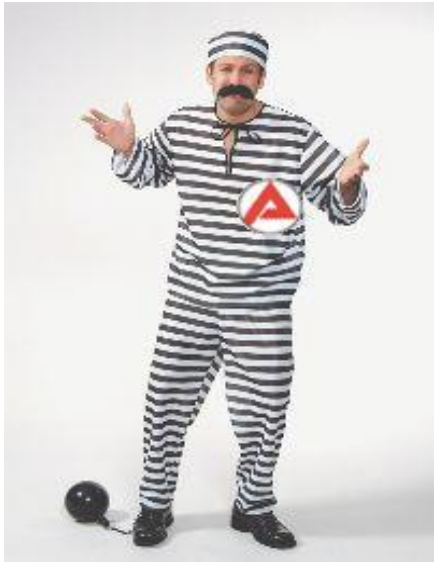
Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Wie sieht er aus – der typische Social Engineer?



Der Meister selbst: Kevin Mitnick

Ihr erster Kontakt mit einem Social Engineer

RÜHLCONSULTING

Wer war der erste Social Engineer, mit dem Sie Kontakt hatten?

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Motivation und Ziele eines Social Engineers

RÜHLCONSULTING

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Welche Informationen sind für einen Angreifer nützlich?

Telefonlisten / Mitarbeiterlisten
Organigramme und Hierarchiestrukturen
Dienstleister und Zulieferer
Raumpläne
Dienst-, Schicht- und Urlaubspläne
Memos und Briefe
Netzpläne, Computernamen, Netzwerkadressen
Funktionsweise von Zugangskontrollsystemen
Prozessbeschreibungen (insbesondere aus dem Bereich des IT-Supports)
Arbeitsanweisungen und Policies
mangelnd sicher entsorgte Datenträger

DEUTZ - FAHR - Vertragshändler

Traktoren, Mähdrescher & Erntemaschinen
Landwirtschaftliche Maschinen & Geräte
Hoftracs, Radlader & Teleskoplader
Baumaschinen- & Motorentechnik
Melk-, Kühltechnik & Notdienst
Kommunaltechnik, Zentralersatzteillager
Reifenservice, Mietgeräte & Leihtraktoren

HEINZ PIEPER LANDTECHNIK
Inhaber: Heinz-Josef Pieper

Hauptbetrieb: Filialbetrieb:
Anhc
4645

AKTUELLE TELEF

Hier Ihre persönlichen

Geschäftsleitung:	**Heinz-Josef Pieper, Georg Pieper**
Zahlungsverkehr, Buchhaltung u. Fachbereich für Melktechnik	**Georg Pieper**
Sekretariat, Rechnungswesen:	**Beate Westerhoff u. Sonja Leiting**
Verkaufsleiter Landtechnik:	**Heinz-Josef Pieper**
Verkaufsberater Landtechnik:	**Carsten Graaf**
Fachbereich Melk- u. Kühltechnik	**Hermann Terhorst**
Computerfütterung:	**Thomas Fenners Nick Bielefeld**
Ersatzteillager Millingen Lagerleitung Thekenverkauf	**Vinzenz Köster Ricardo Kunath**
Technik Millingen Werkstattleitung/-meister stellv. Werkstattleitung/-meister Getriebetechniker: Geselle: Geselle: Geselle:	Rep.-Annahme: **Georg Schlaghecken Jan Büdding Hermann-Josef Bauer Heiner Lohmann Gerhard Harks Marcus Ehringfeld**
Technik Drevenack Filialstellenleitung Verkaufsberatung: Geselle: Geselle:	Rep.-Annahme: **Willi Spickermann Rainer Hanzen Thomas Fenners**
Auslieferungsfahrer	**Michael Konnik**
Notdienst-Handy Zur Erntezeit (ständige Erreichbarkeit)	Technikservice sowie Ersatzteile im Notfall **von April bis Novembe**
Homepage - Internet	**www.pieper-landtechnik.de**
E-Mail - Kontakt	pieper.landtechnik@t-online.de

Mappe2

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI
1	Urlaubsplan 2009/0	09.07.2009 10:17																																	
2			1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31		
3	Abteilung 4		Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa
4	Muster 1 Ulricke																																		
5	Muster 2 Ludwig																																		
6	Muster 32 Annette																																		
7																																			
8	Abteilung 12																																		
9	Muster 20 Gunnar																																		
10																																			
11	Abteilung 13																																		
12	Muster 4 Bettina																																		
13	Muster 5 Andrea																																		
14	Muster 6 Nadine																																		
15	Muster 8 Samira																																		
16	Muster 9 Marion																																		
17	Muster 11 Aline																																		
18	Muster 33 Ulrike																																		
19	Muster 34 Officeleitung																																		
20																																			
21	Abteilung 16																																		
22	Muster 7 Kerstin																																		
23	Muster 10 Sandra																																		
24																																			
25	Abteilung 18																																		
26	Muster Anja																																		
27	Muster 12 Heike																																		
28																																			
29	Abteilung 20																																		
30	Muster 13 Christiane																																		

Ergebnis / Tabelle2 / Tabelle3

Wie werden die Informationen beschafft?

RÜHLCONSULTING

Trashing / Dumpster Diving
Über das Telefon
Vor Ort
Informationsquelle Öffentlichkeit
- Internet / Suchmaschinen
- In der U-Bahn / im Zug
- Auf Festen (->“Bierlaune“)

Technische Hilfsmittel
- Keylogger
- Spyphones
- Kameras
- Mikrofone / Richtmikrofone

RÜHLCONSULTING

Tarnung

Verkleidung
(z.B. Uniform der Sicherheitsfirma, das Brustschild der Reinigungsfirma oder ein Blaumann mit Werkzeugkiste)

Die „Sprache“ des Opfers beherrschen

- Ansprache im Unternehmen („Du“ oder „Sie“)
- Abkürzungen (z.B. Abteilungsbezeichnungen)
- *„Firmenspezifisches Fachchinesisch“*

Angriffsformen

Die verschiedenen Typen von Angreifern (social)

- Angriff auf „Vertrauensbasis“
- Der „Hilfsbedürftige“
- Der „Moralische“ / Erzeugen von Schuldgefühlen
- Der „Insider“
- Der „Fachchinese“
- Der „Vorgesetzte“

Kombination mit technischen Angriffsformen (technical)

- Phishing
- Präparierte Internetseiten
- E-Mail – Anhänge
- Popup-Fenster
- „verlorene“ Wechselmedien (z.B. USB-Sticks)

RÜHLCONSULTING

Aus der Praxis

„verlorene“ USB-Sticks

Terroranschläge in London

news 12.06.2006 12:28

heise Security

USB-Sticks als Trojanische Pferde der Neuzeit

In der griechischen Sage übertölpelte Odysseus die Einwohner Trojas noch mit einem vermeintlich zurückgelassenen, hölzernen Pferd. Seine Nachfolger arbeiten immer noch erfolgreich nach dem gleichen Prinzip: E-Mails mit angeblichen Nacktbildern – oder auch scheinbar verlorene USB-Sticks. Steve Stasiukonis von Secure Network Technologies **berichtet[1]** über einen interessanten Einbruchstest bei einer Kreditgenossenschaft, bei dem er über speziell präparierte USB-Sticks mehr interessante Daten in seinen Besitz bringen konnte, als er zu hoffen wagte.

Im Auftrag der Finanzexperten sollte Stasiukonis die Sicherheit des Netzes testen und dabei insbesondere auch in seine Social-Engineering-Trickkiste greifen. Anstatt mit den üblichen Schauspielertricks beim Smalltalk oder Flirt ein paar Informationen abzustauben, präparierten Stasiukonis und seine Mitarbeiter USB-Sticks unter anderem mit einem Keylogger, der Passwörter ausspionierte und dann per E-Mail verschickte. Von diesen modernen Trojanischen Pferden "verlor" Stasiukonis zwanzig auf dem Firmengelände. Die Angestellten konnten der Versuchung natürlich nicht widerstehen: Fünfzehn wurden gefunden und vom glücklichen Finder auch prompt in Firmenrechner gesteckt.

Ob für die anschließende Aktivierung des Keyloggers der Autorun-Mechanismus zum Einsatz kam oder die Angestellten aus Neugier die gefundenen Applikationen von Hand starteten, lässt sich dem Artikel zwar nicht entnehmen. Man darf aber wohl getrost annehmen, dass auch Letzteres passieren würde, wenn es der Angreifer geschickt genug anstellte.

Aus der Praxis

Quelle: Trendmicro

14.07.2005

Neue Social Engineering-Techniken im Einsatz: Menschliche Tragödien sollen Neugierde wecken

Neuer Trojaner lockt mit Videoaufnahmen vom Terror-Anschlag in London

TREND MICRO (Nasdaq: TMIC, TSE:4704) hat mit TROJ_DONBOMB.A einen Trojaner identifiziert, welcher den aktuellen Bomben-Terror in London als Grundlage seiner Social Engineering-Technik verwendet. Der Trojaner verbreitet sich via eMail und enthält eine gefälschte Absenderadresse des Nachrichtensenders CNN. Im Textkörper wurde eine modifizierte HTML-Kopie der CNN-Webseite eingefügt, der Anhang verspricht Amateuraufnahmen des tragischen Vorfalls von vergangener Woche.

Der Trojaner TROJ_DONBOMB.A verwendet Social Engineering-Techniken, die in der jüngsten Vergangenheit auch bei anderer Malware immer häufiger zu beobachten sind: Um höhere Infektionsraten zu erreichen, täuschen die eMails vor, dass sie von einer bekannten und seriösen Nachrichtenagentur versendet wurden.

Die Verwendung eines konkreten und aktuellen Anlasses ist eine sehr bekannte und oft verwendete Methode bei Virenschreibern. Relativ neu ist aber das Vortäuschen der infizierten eMails, von einer bekannten Nachrichtenagentur abzustammen. Die Vermutung liegt nahe, dass diese Methode in Zukunft immer mehr an Bedeutung gewinnen wird.

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Wie erkenne ich einen Social Engineer

Die schlechte Nachricht zuerst:

Es gibt kein Patentrezept! ☹

Es gibt keinen Patch für menschliche Dummheit!

Verhaltenstipps bei Anfragen einer nicht-verifizierten Person

Prüfung, ob die Person tatsächlich der- oder diejenige ist, für die sie sich ausgibt

- Rufidentifikation / Abgleich mit internem Telefonverzeichnis
- Rückruf
- Bürgschaft einer vertrauten Person
- Rückversicherung beim Vorgesetzten des Antragstellers
- eindeutige Identifikation anhand der Stimme
- In Person mittels eines Ausweises

Feststellung, ob der Antragsteller gegenwärtig bei der Firma angestellt ist oder die Beziehung solcherart ist, dass ein berechtigter Wissensbedarf besteht

- Nachschlagen im Mitarbeiterverzeichnis
- Verifikation über den Vorgesetzten oder einen Kollegen der Abteilung

Bestimmung, ob die Person dazu autorisiert ist, diese spezielle Information zu erhalten oder die gewünschte Handlung ausgeführt zu bekommen

- Einholen der Erlaubnis vom Vorgesetzten
- Freigabe durch den Eigentümer der Information

Verhaltenstipps bei Anfragen einer verifizierten Person

Festestellen, ob die Firma diese Person gegenwärtig beschäftigt oder eine Beziehung zu ihr hat die es ihr gestattet, Zugang zu den geforderten Informationen zu erlangen

Prüfen, ob diese Person zur Kenntnis der angefragten Information oder Handlung berechtigt ist

Passwörter


Hello Guys
The password
for the computer
has changed it is
now: XLP274 !
2008/04/15 14:03

Generelle Tipps

Beim Verlassen des Raumes den Bildschirm des PCs sperren

Zugangsdaten zu Systemen nicht notieren oder schriftlich festhalten

Datenklassifizierung beachten oder, bei Nichtvorhandensein: eigene „Regeln“ aufstellen (öffentlich, intern, vertraulich/geheim) und Informationen demgemäß behandeln

Vertrauliche Unterlagen bei Abwesenheit grundsätzlich verschlossen aufbewahren

Vertrauliche Unterlagen generell sicher entsorgen (Papier in den Schredder, Datenträger durch spezielle Wipe-Programme löschen, etc.)

Beim Verlassen von Meetingräumen alle schriftlichen Aufzeichnungen (Flipchart, Whiteboard, etc.) entfernen und sicher verwahren

Mobiltelefone und PDAs wie den Arbeitsplatz-PC mit einem Passwort schützen

Motivation und Ziele dieses Vortrags

Social Engineering – was ist das überhaupt?

Welche Formen des Social Engineering gibt es?

Wie sieht der typische Social Engineer aus?

Motivation und Ziele eines SE

Vorgehensweise eines SE

Wie erkenne ich SE-Angriffe und wie schütze ich mich davor?

Fazit, Fragen & Diskussion

Die wichtigste Regel

RÜHLCONSULTING

- Es gibt kein „Schema F“ zur Erkennung
- Sei kritisch und hinterfrage die Dinge
- Betrachte nichts als selbstverständlich

Literaturhinweise und Empfehlungen

RÜHLCONSULTING

- Kevin Mitnick *** Die Kunst der Täuschung (ISBN-13: 978-3826615696)
- Kevin Mitnick *** Die Kunst des Einbruchs (ISBN-13: 978-3826616228)
- Jens Eichler *** „Trau, schau, wem“ (<KES> 2007*1)
  (http://www.auditor24.net/TrauSchauWem.pdf)

- Ein ehrenwerter Gentleman (DVD, Amazon-ASIN: B0000AGF7Z)
- 666 - Traue keinem, mit dem du schläfst (DVD, Amazon-ASIN: B00006L9R1)
- Takedown (DVD, Amazon-ASIN: B00008XQHK)


THANK
YOU

Nochmal … die **WICHTIGSTE** Regel

RÜHLCONSULTING

- Es gibt kein „Schema F“ zur Erkennung
- Sei kritisch und hinterfrage die Dinge
- Betrachte nichts als selbstverständlich

Nicht alles ist wirklich immer das, was es auf den ersten Blick zu sein scheint !!!

RÜHLCONSULTING

RÜHLCONSULTING

Vielen Dank!!

Welche Fragen haben Sie noch?

RÜHLCONSULTING

Wenn nach dem Vortrag Fragen auftauchen:

RÜHLCONSULTING GmbH
Neumeyerstraße 48
90411 Nürnberg
Mail@RUEHLCONSULTING.de
Telefon 0911.47 75 28-0
Telefax 0911.47 74 28-49

Jens.Eichler@RUEHLCONSULTING.de
Telefon 0911.47 75 28-33
Telefax 0911.47 75 28-4933