BenutzerInnen im Spannungsfeld

IT-Gefahren
IT-Vorfälle
Praktische Erfahrungsbeispiele

Manfred Holzbach

A-SIT

Zentrum für sichere Informationstechnologie-Austria

Themen

- Spektakuläre Vorfälle aus der letzten Zeit
  Österreich: CEO Fraud -50 Mio € Schaden
  Nationalbank Bangladesh: komplexer Angriff: -100 Mio US$ Schaden
- Top-Gefährdungen:
  Ransomware, Phishing
- Passwortsicherheit
  Statistik, Demo
- Verhalten auf Reisen
- Fazit, Diskussion: Werden wir BenutzerInnen überfordert ?

A-SIT

Inhalte meines Vortrags

- Erfahrungswerte aus der Praxis
- Erörterung:
  - *BenutzerInnen als Werkzeuge für Angriffe*
  - *Mißbrauch des guten Glaubens*
  - *Wie sowohl komplexe aber auch ganz einfache Angriffe Strukturschwächen und Routine ausnützen*
  - *Die Gefahr wird oft unterschätzt – am Beispiel von Passwörtern und Dienstreisen*

A-SIT

Anliegen meines Vortrags

- Kein erhobener Zeigefinger
- Angebot zum Mit- und Nachdenken
- Der Gegner ist schon da
  - „Es kann jeden immer und überall treffen“
  - „Richtig vorsorgen aber auch richtig reagieren“
- -“es gibt nichts was es nicht gibt“

CEO-Fraud: Luftfahrt-Zulieferer

Die Mail kam von ganz oben, vom Vorstandschef persönlich. Unter dem Siegel der strengsten Verschwiegenheit wurde eine Mitarbeiterin eines österreichischen Luftfahrtzulieferers während der Weihnachtstage angewiesen, 50 Millionen zu überweisen. Das Geld, so stand es in der Nachricht, sollte für eine geheime Firmenübernahme im Ausland verwendet werden. Also: geheime Kommandosache, kein Wort zu niemandem..

Die Mitarbeiterin tat, wie ihr geheißen. Und transferierte die 50 Millionen Euro offensichtlich auf Konten im Ausland.

Quelle: Die Presse, NEWS

A-SIT

CEO-Fraud: Luftfahrt-Zulieferer

50 Millionen sind weg. Die Spur des Geldes verliert sich laut jüngsten Meldungen in der Slowakei und in Asien, die Wiener Wirtschafts- und Korruptionsstaatsanwaltschaft ermittelt.

…stellt sich allerdings auch die Frage, wie eine Mitarbeiterin überhaupt derart hohe Summen bewegen konnte? Denn die Angestellte soll im Besitz der Zugangsberechtigungen zweier Vorstände gewesen sein.

A-SIT

Quelle: Die Presse, NEWS

CEO-Fraud: Luftfahrt-Zulieferer

Folgen:
Fehlbetrag verfünffacht
Finanzchefin, CEO und AR Vorsitzender wurden gefeuert
Aktienkurs hat sich bis heute nicht erholt

50 Mio mit einer E-Mail ! ?

Quelle: Die Presse, NEWS

A-SIT

CEO-Fraud

Fehlverhalten war „nur“ der Anlass.
Die Ursachen sind strukturell:

- Strenge Hierachien ⇨ unbedingter Gehorsam
- Leichter Zugang zu Unternehmensinformationen
- Keine Zweifel an Mitteilungen der Unternehmensleitung
  Mails vom höchsten Chef werden nicht hinterfragt
- Offensichtliche „Kultur“ nicht näher begründeter Geheimhaltungen
- Offenbar de-facto Alleinzeichnungsberechtigung

A-SIT

CEO-Fraud

Der Versand solcher Betrugs-E-Mails kann kaum verhindert werden.

Die Betrüger verschleiern ihre Identität und Herkunft und können bei Bedarf jederzeit die Adresse wechseln.

⇨ Sensibilisierung des Personals besonders in für Betrüger notwendigen Positionen (Buchhaltung, Finanz, ..)

⇨ Bei ungewöhnlichen / zweifelhaften Kontaktaufnahmen keine Information herausgeben und keine Anweisungen befolgen, auch wenn man unter Druck gesetzt wird.

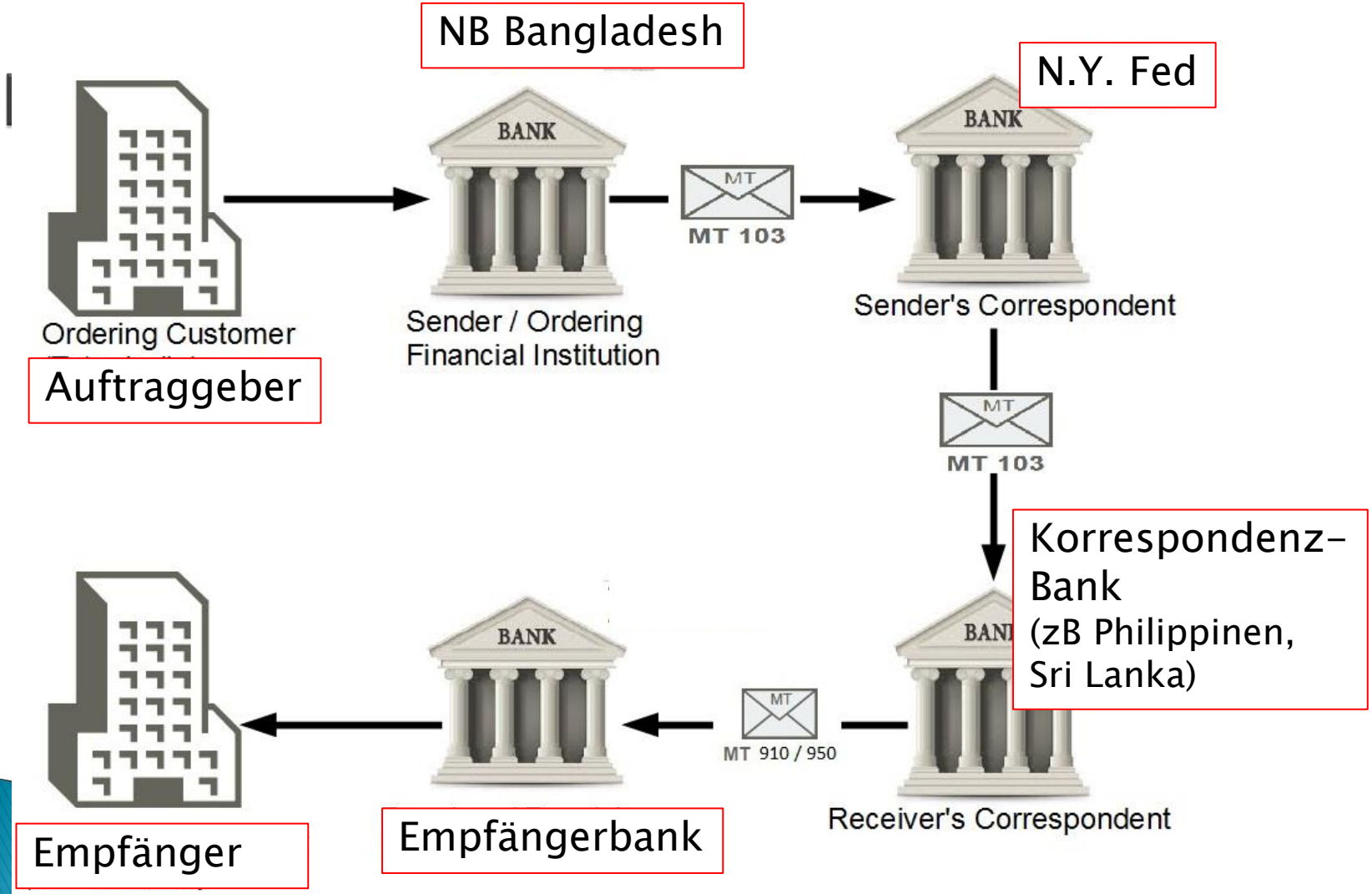
⇨ Vieraugenprinzip mit Kollektivunterschrift für Überweisungen.

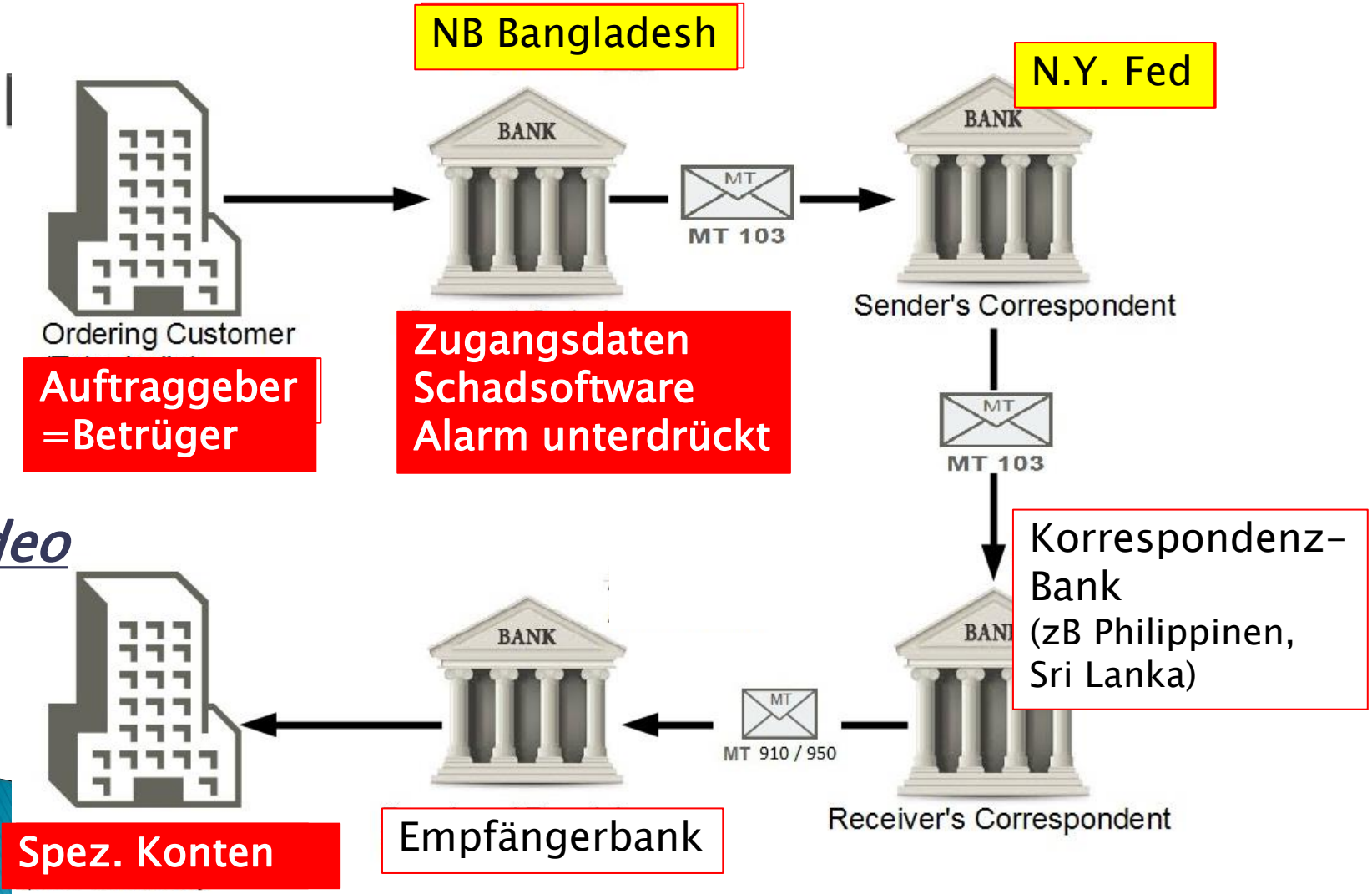
Quelle: MELANI (CH)

Komplexer Angriff: NB Bangladesh

- Missbrauch des globalen SWIFT Bankennetzwerks
- Beispiel für strategisch geplanten, gezielten Angriff
- Schaden fast 100 Mio US$, um ein Haar weitere 900 Mio
- Kombination aus:
  Nutzung lokaler Schwachstellen
  Spezielle eingeschleuste Schadsoftware
  Strukturelle weltweite Schwächen

A-SIT


NB Bangladesh
N.Y. Fed
BANK
MT
MT 103
Ordering Customer
Auftraggeber
Sender / Ordering
Financial Institution
Sender's Correspondent
MT
MT 103
Korrespondenz-
Bank
(zB Philippinen,
Sri Lanka)
BANK
MT
MT 910 / 950
Receiver's Correspondent
Empfängerbank
Empfänger


NB Bangladesh
N.Y. Fed
BANK
MT
MT 103
Ordering Customer
Auftraggeber
=Betrüger
Zugangsdaten
Schadsoftware
Alarm unterdrückt
Sender's Correspondent
MT
MT 103
Korrespondenz-
Bank
(zB Philippinen,
Sri Lanka)
Video
BANK
MT
MT 910 / 950
Receiver's Correspondent
Spez. Konten
Empfängerbank

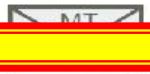
NB Bangladesh

N.Y. Fed

START

Ordering Customer

Auftraggeber
=Betrüger



MT 103

Sender's Corre

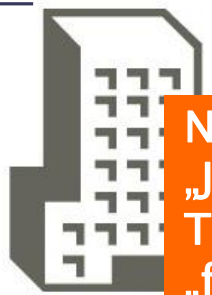
Zugangsdaten
Schadsoftware
Alarm unterdrückt

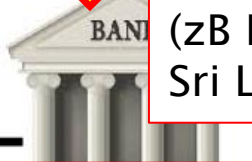
Führt TX automatisch durch
Wochenende:
Niemand erreichbar

103

Korrespondenz-Bank
(zB Philippinen,
Sri Lanka)

Video



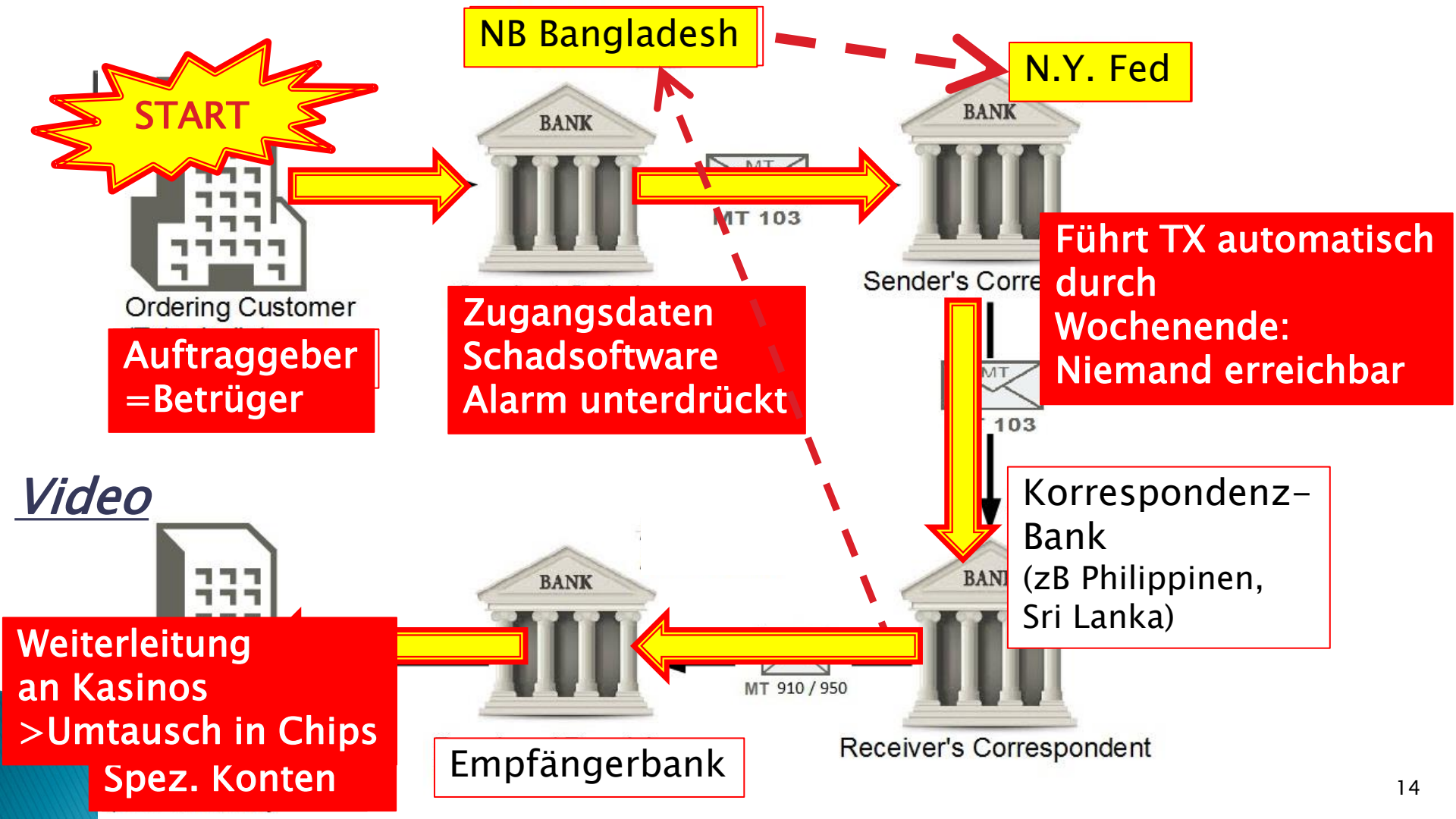


Namensgleichheit:
„Jupiter“ auf Iran-Sanktionsliste
Tippfehler:
„fandation“ statt „foundation“

Sri Lanka, DeuBa schöpfen Verdacht
Stoppen „ihre“ Weiterleitung

Spez. Konten

Empfängerbank


NB Bangladesh
N.Y. Fed
START
BANK
MT 103
BANK
Sender's Corre
Führt TX automatisch durch
Wochenende:
Niemand erreichbar
Ordering Customer
Auftraggeber
=Betrüger
Zugangsdaten
Schadsoftware
Alarm unterdrückt
MT
103
Video
Korrespondenz-
Bank
(zB Philippinen,
Sri Lanka)
BANK
BANK
MT 910 / 950
Weiterleitung
an Kasinos
>Umtausch in Chips
Spez. Konten
Empfängerbank
Receiver's Correspondent

Komplexer Angriff: NB Bangladesh

32 Schwachstellen in der NB ausgespäht
Offenbar gültige Zugangsdaten erbeutet

Schadsoftware, speziell auf „SWIFT Alliance Access“ zugeschnitten:
Verschleiern von Transaktionen
Unterbinden zwingenden Ausdrucks von Bestätigungen

➔ 4.Februar 2016: Wochenende und islamische Feiertage
➔ Auslösen gefälschter Transaktionen 951 Mio US$ via N.Y. Fed an private Konten auf Philippinen, Sri Lanka

Quellen: BAE Systems, Reuters

Komplexer Angriff: NB Bangladesh

- 81 Mio US-$ sind weg
  - in Spielbanken verschwunden
- 20 Mio US-$ von Sri Lanka rechtzeitig gestoppt
- 850 Mio US-$ wegen Formalfehlern nicht durchgeführt

Der Finanzminister Bangladeshs erfährt davon erst aus der Zeitung

Gouverneur Atiur Rahman muss zurücktreten

Quellen: BAE Systems, Reuters

Komplexer Angriff: NB Bangladesh

32 Schwachstellen in der NB ausgespäht
Offenbar gültige Zugangsdaten erbeutet

Schadsoftware, speziell auf „SWIFT Alliance Access“ zugeschnitten:
Verschleiern von Transaktionen
Unterbinden zwingenden Ausdrucks von Bestätigungen

➔ 4.Februar 2016: Wochenende und islamische Feiertage
➔ Auslösen gefälschter Transaktionen 951 Mio US$ via N.Y. Fed an private Konten auf Philippinen, Sri Lanka

Quellen: BAE Systems, Reuters

NB Bangladesh: Aufarbeitung

Wer ist schuld ?

Lokale Ursachen:

- Hilfe durch Insider ? (keine Infos darüber)
- Leerer Drucker zwar als ungewöhnlich erkannt, offenbar häufige technische Probleme damit
- Einschleusen der Malware offensichtlich mit Routine möglich,
  ähnliche Angriffe in Vietnam und Ecuador
- Wieso keine Echtzeit-Kontrollen vor Ort bei derart hohen Beträgen ?

A-SIT

NB Bangladesh: Aufarbeitung

Wer ist schuld ?

Strukturelle Ursachen:

- N.Y. Fed und SWIFT wollen nichts falsch gemacht haben, dennoch:
- „Finale“ Durchführung in Echtzeit, aber keine wirksamen Echtzeit-Kontrollmechanismen ?
- Überweisungen von Notenbanken auf Konten privater Empfänger sind eigentlich ungewöhnlich, vor allem bei höheren Beträgen.

A-SIT

NB Bangladesh: Aufarbeitung

Was bleibt ?

- Bangladesh hat den „Schwarzen Peter“
- alle nachgeordneten Banken sowie SWIFT haben darauf vertraut und können ihre Compliance darstellen, auch wenn sie sich als unwirksam herausgestellt hat.
- Zurück bleibt enormer Schaden und massive Geldwäsche.
- Philippinen kommen auf die „Schwarze Geldwäsche Liste“

A-SIT

Komplexer Angriff: NB Bangladesh

- *Epilog:*
- SWIFT und New York Fed im Kreuzfeuer der Kritik
- Untersuchungen FBI, Dep.of Justice, US-Kongress
- Reuters Report spricht von “Unordnung und Pfusch” (disarray and bungling) bei den involvierten Banken, namentlich N.Y.Fed.
- $101 Mio durchgeführt, obwohl auffällig unübliche (an Personen) und tw. fehlerhaft formatierte Aufträge. Nur $20 Mio davon konnten zurückgeholt werden.
- Durchführung der ganzen $951 Mio *an Zufall gescheitert.*
- SWIFT bietet “Sicherheitsberatung” an.

A-SIT

Links zu Bangladesh-Attacke

- https://www.heise.de/newsticker/meldung/Milliarden-Coup-in-NY-Zentralbank-Konto-per-Ueberweisung-geleert-3131832.html
- http://www.reuters.com/investigates/special-report/cyber-heist-federal/
- http://www.smh.com.au/business/banking-and-finance/printer-error-foiled-billiondollar-bank-heist-20160317-gnljm4.html

Erpressung durch Ransomware

Das von einem Erpressungstrojaner betroffene Krankenhaus Hollywood Presbyterian Medical Center in Los Angeles hat seine IT-Systeme mit einer Lösegeldzahlung freigekauft. ..

40 Bitcoins (=ca 24000 €) sollen bezahlt worden sein.

Krankenhäuser sind besonders beliebte Ziele:
Betriebsunterbrechung kann
verheerende Folgen haben

Quelle: heise.de

Ransomware aktuell: Goldeneye

Der Verschlüsselungstrojaner Goldeneye, der seit 6.12. 4 Uhr in Deutschland wütet, zielt direkt auf Personalverantwortliche in Firmen. Die Drahtzieher scheinen im großen Stil Daten über deren Mailadressen und offene Stellen abgegriffen zu haben.

- Mails enthalten eine infektiöse XLS-Datei mit Makros und

Er sucht sich gezielt Personalabteilungen als Opfer.
Die E-Mails mit dem Schadcode im Anhang nehmen dabei Bezug auf tatsächlich offenen Stellenausschreibungen der jeweiligen Firma.

XLS-

aher

Die Mails sind in fehlerfreiem Deutsch verfasst und verwenden eine korrekte Anrede, die zu der Zieladresse passt..

GIT

Erpressung durch Ransomware

- Verschlüsselungstrojaner (z.B. TeslaCrypt) landen in der Regel als E-Mail-Anhang auf Computern und verschlüsseln Teile des Systems.
- In großen IT-Netzwerken wie beispielsweise in einem Krankenhaus können davon alle Daten betroffen sein, die der Schädling über das Netz erreicht
- Ohne den zur Entschlüsselung nötigen privaten Krypto-Schlüssel sind die Daten meist verloren.

A-SIT

Quelle: heise.de

Ransomware aktuell: Goldeneye

- Absender oft „Rolf Drescher“;
  Racheakt an Dipl.- Ing. Rolf B. Drescher VDI & Partner;
  bietet Entschlüsselungshilfe für Opfer des Trojaners Petya an .
- Mails enthalten eine infektiöse XLS-Datei mit Makros und einen echt aussehenden PDF-Lebenslauf, der auf die XLS-Datei verweist.
- Daten stammen vermutlich von Jobbörsen und sind daher echt.

Quelle: heise.de

Ransomware aktuell: auch an mich…

A1 Online-Rechnung

Betreff: A1 Online-Rechnung
Von: A1 Online <leventkurban@ipfsbroker.com>
Datum: 07.12.2016 14:42
An: <manfred.holzbach@a-sit.at>

Mein Verhalten war:

? Verdächtiger Absender

? Verdächtiger Inhalt

Verbindungsentgelte: 183.43 EUR

Verbrauchtes Datenvolumen:

? Verdächtige Sprache

Ansicht einer Rechnung

Dennoch: Glück gehabt,
Nicht abgelenkt,
Eher schlecht gemachte Mail

Erpressung durch Ransomware

Bezahlen oder nicht bezahlen ?

- Keine Garantie für tatsächliche Entschlüsselung
- Im Sinne ihres „Marketing“ liefern die meisten Erpresser nach Lösegeldzahlung
- Preise werden „kundengerecht“ kalkuliert, Recovery kommt oft teurer, wenn es überhaupt funktioniert.

Bezahlen finanziert neue Erpressungen

Ransomware: Was (nicht) tun:

- Regelmäßige Backups auf externe Datenträger; mehrere Generationen (A, B, Monatskopien)
- Absender, Inhalt und Sprache auf Auffälligkeiten kontrollieren.
- (mail-) Virenschutz, Spam Filter aktuell halten.
- Nicht drauf los klicken.
- Melden (Polizei), vor allem wenn man darauf hereingefallen ist.

Aber: Mails werden immer besser

Es ist keine Schande !

A-SIT

Links zu Ransomware

- BSI Themenpapier und Lagedossier
  https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/Ransomware/Ransomware_node.html

Phishing

- Betrüger versuchen, über gefälschte Internetseiten, E-Mail oder Kurznachrichten an persönliche Daten zu gelangen.
- Zum Beispiel um das Konto zu plündern Demo-Video
- Typisch für Phishing ist die Nachahmung des Designs einer vertrauenswürdigen Stelle.

Quelle: KTipp (CH)

Phishing: B

- Sparkasse
- Raiffeisen
- Post (SMS)
- BMF

Am 26. Okt. 2016, um 03:16, Raiffeisen Bank <
no_reply@raiffeisen.at> schrieb:

Bestätigung Ihrer Daten erforderlich! Konto eingeschränkt. Datum: 03.11.2015

Sehr geehrter Kunde,

wir, das Sicherheitscenter der **Raiffeisen Bank International AG**, sind stets bemüht Ihnen ein sichereres Zahlungsnetzwerk zu bieten.

Aus diesem Grund hat unser Raiffeisenbank-Sicherheitsteam für unsere Kunden ein neues Sicherheitszertifikat für Mobile Endgeräte entwickelt. Nur so können wir Missbrauch durch Dritte ausschließen und Sie vor einem finanziellen Schaden bewahren. Die Installation ist nur einmal notwendig, erneute Sicherheitsupdate für ihr Endgerät werden fortan automatisch ausgeführt.

Sollten Sie dieser Aufforderung nicht nachkommen, sind Sie im Betrugsfall voll haftbar, des Weiteren werden wir nach Ablauf einer **Frist von 14 Tagen** vorsorglich Ihr Konto sperren.

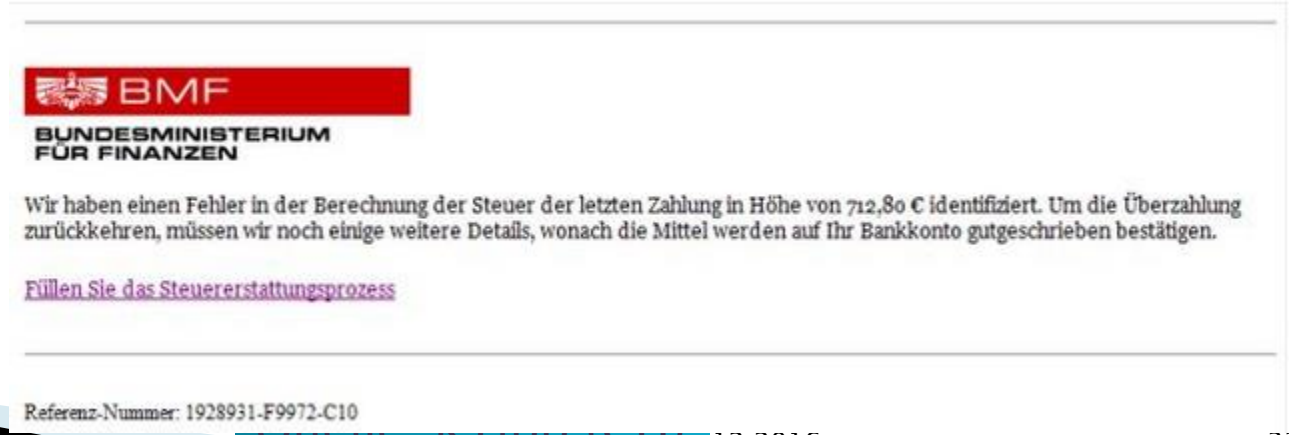
Fälschung

Mit freundlichen Grüßen
Ihr Kundenservice

Impressum 7.7.5 © Raiffeisen

Phishing: Beispiele

- Sparkasse
- Raiffeisen
- Post (SMS)
- BMF



Quelle: KHpp (CH)

Phishing: Was (nicht) tun:

- Banken, Post, Behörden fragen niemals per SMS nach Zugangsdaten
  Aber: Marketing-Mails mit Fragen
- Absender, Inhalt und Sprache auf Auffälligkeiten kontrollieren.
  Nicht drauf los klicken
- Virenschutz, Spam Filter aktuell halten.
- Apps nur aus offiziellen Stores herunterladen.
- Melden (Hotlines), vor allem wenn man darauf hereingefallen ist.
  Es ist keine Schande !

A-SIT

Evergreen Passworte:
SFG Richtlinie EDV-Nutzung

- *Das initiale Passwort ist bei erstmaliger Anmeldung von der Benutzerin/dem Benutzer sofort zu ändern. Folgende Anforderungen müssen erfüllt werden:*
- Windows-Login-Passwörter müssen aus mindestens 8 Stellen bestehen.
- Windows-Login-Passwörter müssen eine Kombination aus 3 von 4 möglichen Zeichengruppen (numerische Zeichen, Großbuchstaben, Kleinbuchstaben, Sonderzeichen) darstellen.
- Windows-Login-Passwörter dürfen den BenutzerInnennamen bzw. Teile desselben nicht enthalten.

A-SIT

Passworte: SFG Richtlinie EDV-Nutzung

- Vor- und Nachnamen, Geburtsdaten, Kfz-Kennzeichen, Begriffe aus Wörterbüchern und/oder Lexika, Buchstaben- und Zahlenfolgen (wie z. B. 123456789 oder asdfghjkl) dürfen nicht als Passwörter oder wesentlichen Teilen davon verwendet werden.

#	Count	Ciphertext	Plaintext
1.	1911938	EQ7fIpT7i/Q=	123456
2.	446162	j9p+HwtWWT86aMjgZFLzYg==	123456789
3.	345834	L8qbAD3jl3jioxG6CatHBw==	password
4.	211659	BB4e6X+b2xLioxG6CatHBw==	adobe123
5.	201580	j9p+HwtWWT/ioxG6CatHBw==	12345678
6.	130832	5djv7ZCI2ws=	qwerty
7.	124253	dQi0asWPYvQ=	1234567
8.	113884	7LqYzKVeq8I=	111111
9.	83411	PMDTbP0LZxu03SwrFUvYGA==	photoshop
10.	82694	e6MPXQ5G6a8=	123123
11.	76910	j9p+HwtWWT8/HeZN+3oiCQ==	1234567890
12.	76186	diQ+ie23vAA=	000000
13.	70791	kCcUSCmonEA=	abc123
14.	61453	ukxzEcXU6Pw=	1234
15.	56744	5wEAInH22i4=	adobe1
16.	54651	WqflwJFYW3+PszVFZo1Ggg==	macromedia
17.	48850	hjAYsdUA4+k=	azerty
18.	47142	rpkvF+oZzQvioxG6CatHBw==	iloveyou
19.	44281	xz6PIeGzr6g=	aaaaaa
20.	43670	Ypsmk6AXQTk=	654321
21.	43497	4V+mGczxDEA=	12345
22		p2K	666666
23		dJY w==	sunshine
24.	34963	1McuJ/7v9nE=	123321
25.	334	xPIsF n	

Netzpiloten.de Pressetext.com

Q: Adobe Q: Splashdata/PC magazin

Rang	Passwort
1	123456
2	password
3	12345678
4	qwerty
5	12345
6	123456789
7	football
8	1234
9	1234567
10	baseball
11	welcome
12	1234567890
13	abc123
14	111111
15	1qaz2wsx
16	dragon
17	master

Passwort-Demo:

- Grundlagenversuch: Brute Force Attacke auf 4 Stellen
- Was leisten 8 Stellen ?
- Warum nicht aus Wörterbuch ?
- Was bringt Änderung und Sperre ?
- Kann man Passworte sicher verwahren ?

A-SIT

Passwort-Demo:

1. PDF Datei erstellen
2. Passwortschutz (Zuruf; wegen Zeitlimit 4 Stellen)
3. Brute-Force Angriff darauf
4. Passwortschutz 8 Stellen aus Wörterbuch
5. Brute-Force Angriff darauf
6. Schätzungen für 12 oder mehr Stellen (1 PC)
7. Schlussfolgerungen auf Bot-Netz-Attacken

A-SIT

Passwort-Demo:

1. PDF Datei erstellen
2. Passwortschutz (Zuruf; wegen Zeitlimit 4 Stellen)
3. Brute-Force Angriff darauf
4. Passwortschutz 8 Stellen aus Wörterbuch
5. Brute-Force Angriff darauf
6. Schätzungen
7. Schlussfolger

https://apps.cygnius.net/passtest/

Das ist ein Passworttester, der zwar nicht sonderlich schön ist, aber Wörter, Phrasen etc. berücksichtigt für die Kalkulationszeit.

https://www.betterbuys.com/estimating-password-cracking-times/

Live Brute-Force Schätzung u Entwicklung über die Jahre

Passworte: SFG Richtlinie EDV-Nutzung

- BenutzerInnen-Passwörter laufen alle 60 Tage ab und müssen daraufhin erneuert werden.
- Das gleiche BenutzerInnen-Passwort darf erst bei der vierten Passwortänderung wiederverwendet werden.

Passwort: Änderungszwang in Diskussion

- Wissenschaftliche Diskussion ob erzwungener Wechsel *von nicht kompromittierten* Passwörtern mehr Sicherheit bringt.
- Pro: Begegnen von alf. Passwort-Diebstahl (Zettel, Keylogger,…)
- Kontra: Gefahr, dass Qualität der Passwörter insgesamt sinkt.
- Frage: Ist mein Passwort kompromittiert oder nicht ?

Vergleich:
Würde man ein intaktes physisches Türschloss immer wieder vorsorglich auswechseln?

Q: ISB (CH) | Q: Studie Univ. Ottawa | Q: Studie Univ. North Carolina

Passwort: Änderungszwang in Diskussion

- Angreifer werden nicht warten, bis das Passwort möglicherweise ersetzt wird, d. h. der Angriff wird unmittelbar nach der Kompromittierung stattfinden.
- In vielen Angriffsszenarien ist Kenntnis des Passworts im Klartext nicht erforderlich: etwa an „Pass-the-Hash“-Angriffe
- Sinnvoll sind jedenfalls intensive detektive Maßnahmen, um kompromittierte Passwörter festzustellen.
- z. B. dass man BenutzerInnen immer informiert, wann sein/ihr Passwort zuletzt verwendet worden ist. Entsprechend sensibilisierte BenutzerInnen werden dann Missbräuche erkennen.

A-SIT

Passworte: SFG Richtlinie EDV-Nutzung

- Ein 10-maliger Login-Versuch mit falschem Passwort führt zur Sperre des BenutzerInnenaccounts. …

Damit kann man Angriffen via Benutzer-Passwörtern begegnen

Beim Administrator würde das System lahmgelegt werden
Auch die Sperre kann gehackt werden

Passwort-Praxis / Statisitik

- http://www.pc-magazin.de/news/schlechteste-passwoerter-2015-top-liste-report-studie-3195624.html

- http://stricture-group.com/files/adobe-top100.txt
- http://www.netzpiloten.de/die-25-haufigsten-passworter-und-pins/
- http://www.pressetext.com/news/20161108035

- https://gborn.blogger.de/stories/857906/ (Wiederherstellung gesperrter PW)
- http://de.wikihow.com/Ein-passwortgesch%C3%BCtztes-Computer-Benutzerkonto-hacken
- http://www.pcwelt.de/ratgeber/Vergessenes-Passwort-knacken-172191.html

A-SIT

Exkurs: Dienstreisen

Zusammenfassung: Gefährdungen

- Trojaner und Würmer: täglich 350 000 neue

Ausspähen von Daten und Verhalten,
Manipulation, Spam-Versand,
Spionage,
Sabotage (z.B. Verschlüsseln)

Infektion durch:
Phishing
Spam
Drive-By-Download
Datenträger

Nach Angaben des deutschen Branchenverbandes Bitkom tauchen jeden Tag rund 350.000 neue Varianten von Schadsoftware im Internet auf. Die Risiken, seinen Rechner zu infizieren, sind vielfältig und reichen von Trojanern und Würmern über Drive-by-Downloads und Botnetze bis hin zu Spam und Phishing, warnt der Verband und verrät unter Berufung auf einen aktuellen Bericht der European Network and Information Security Agency, was die zehn größten Bedrohungen im Internet sind und wie man sich vor diesen schützen kann.

Zusammenfassung: Gefährdungen

- Trojaner und Würmer: täglich 350 000 neue
- Phishing

Ausspähen von Benutzerdaten
Identitätsdiebstahl (Online Banking, Einkäufe,…)

Zusammenfassung: Gefährdungen

- Trojaner und Würmer: täglich 350 000 neue
- Phishing
- Spam

Weltweit 75% aller Mails unerwünscht
Eingangstor für Schadsoftware
Tarnung wird immer besser
(Rechnungen, Sendungen)

Zusammenfassung: Gefährdungen

- Trojaner und Würmer: täglich 350 000 neue
- Phishing
- Spam
- Erpressung

Sabotage: Ransomware verschlüsselt die Daten
Spionage: Suche nach Geheimnissen oder Peinlichkeiten

Betrifft Privatpersonen, Unternehmen, Prominente, sehr oft Krankenhäuser

A-SIT

Zusammenfassung: Gefährdungen

- Trojaner und Würmer: täglich 350 000 neue
- Phishing
- Spam
- Erpressung
- Denial-of-Service

Botnetze mit >1 Mio PC's entstanden durch Trojaner

Angiff auf A1 Feb 2016:
60 Gbit/s auf Name-Server

Blockieren von IT-Diensten durch „Zuschütten" mit Daten

A-SIT

Diskussion:
Werden wir Benutzerinnen überfordert?

- Informationsflut
- Speed kills:
- Zeitdruck
- 1-Klick Philosophie: Schnell machen, dann korrigieren
- Nerviges:
- Endlose Updates „Bitte schalten Sie nicht aus“
- Aufdringliche Virenscanner etc
- Eigene Schuld
- ….

Wer gewinnt immer ?

Sicherheit Bequemlichkeit

A-SIT

Danke für Ihre Aufmerksamkeit

Manfred Holzbach
Stabsstelle
Zentrum für sichere Informationstechnologie-Austria (A-SIT)

Manfred.holzbach@a-sit.at