

Wolfgang Straßer  
Peter Schwanke



**Live Forensik**

## Firmenportrait

- Juni 2002 gegründet
- inhabergeführt
- Sitz: Leichlingen/Rheinland
  
- Beratungsschwerpunkte:
  - IT-Risikomanagement
    - Business- und IT-Security
    - Business Continuity und Notfallplanung
    - Compliance und Datenschutz
    - Incident Response und Forensik
  
- @-yet IT Security-Akademie
- @-yet Industrial IT-Security GmbH

@-yet GmbH

**IT-  
Risikomanagement**

**Cloud und  
Outsourcing**

**Incident Response  
IT-Forensik**

IT-RESULTING IM FOKUS

# IT-Risikomanagement

Der **bewusste und gezielte** Umgang mit den Risiken,  
die sich für Organisationen  
durch den Einsatz von IT ergeben können!

Sichergestellt werden müssen:

**Integrität,**

**Vertraulichkeit,**

**Verfügbarkeit**

von Prozessen und Daten!

# IT und Risikomanagement

## Aufgaben von IT Risikomanagement:

- Schutz vor Verlust von
    - Know-how
      - Ihr spezielles Firmen Know-how
    - Wertschöpfung
      - Die Firma kann nicht mehr arbeiten wg. IT Ausfall
    - Geld
  
  - Schutz vor Risiken, die sich
    - vertraglich
      - z.B. Kunden-/Lieferantenauflagen etc.
    - gesetzlich
      - z.B. Datenschutzgesetz/IT-Sicherheitsgesetz
- ergeben können.

# @-yet Bausteine IT Risikomanagement

**Business- und IT-  
Security**

**Business Continuity**

**Compliance,  
Datenschutz**

**Incident Response,  
IT-Forensik**

IT-RESULTING IM FOKUS

## Warum Business Security?

- die Risiken nehmen zu
- die Bedrohungslage ist wirklich ernst
- es kann jeden treffen
  
- Oft gehört:
  - Wer interessiert sich für uns?
  - Antwort: der ganze Planet!
  
- Bei uns ist noch nie was passiert!
  - Antwort: das wissen Sie gar nicht!
  
- 100% Sicherheit gibt es nicht!
  - Antwort: stimmt, aber 10-20% sind aber definitiv zu wenig!

➤ Wie wird angegriffen?



## Wie wird angegriffen?

- Hackingangriff von außen
- Informationsbeschaffung von innen
  - Ausnutzen physischer und organisatorischer Schwachstellen - Social Engineering
    - z. B. CEO Fraud
- Datenträgerklau
  - Smartphones, Pads, Notebooks etc.
    - Sind die nicht geschützt.....
- **immer mehr über infizierte und manipulierte**
  - Websites und -shops
  - Portale
  - Cloud
  - APPS und Mobiles

## Aber auch - „Innentäter“

- Whistle-Blower
  - Edward Snowden
  - Julian Assange
  - Chelsea (Bradley) Manning (WikiLeaks)
  - IS-Dokumente
  - Panama Papers
- Systemadministratoren – Neugier!?
- Systemfehler ...
- Sorglosigkeit – Surfen, Downloads, Uploads etc.
- Mitarbeiter – Datenabfluss(-klau)
- etc.

➤ Was so alles geht.....

## Ausgangslage

- Kunde meldet sich bei @-yet:
  - Vorfall vor **2 Tagen**
  - Fast alle Server sind ausgefallen
  - Verdacht auf Verschlüsselungstrojaner
    - Große Teile der Daten sind nicht mehr verfügbar
  - IT-Personal fühlt sich überfordert
    - Gerade läuft Transition-Phase:  
Betrieb beim Dienstleister → neue IT soll übernehmen

- Aufgabenstellungen:
  - Wiederherstellung von Daten
  - Wiederanlauf der IT
  - Bestimmung des Tathergangs
  - Bereinigung der IT



**Interessenskonflikt**

## Zwischenziele

- Sicherung relevanter Systeme, Logs und Spuren
- Feststellen des Zustandes
- Zeit des Vorfalls möglichst genau bestimmen
- Identifikation des Einfallstors
- Identifikation weiterer Angreifer-Tätigkeiten
  
- Sichten von Backups
- Ggf. Wiederherstellung

## Erste Analysen

- Unterschiedliche Varianten:
  - Viele Dateien - mit alter Ransomware verschlüsselt
    - Nicht alle Dateitypen
  - Es gibt leere Partitionen mit dem Namen einer 2. Ransomware
  - Terminalserver wurde zu 20% mit Nullen überschrieben
  - RAID's der Backup-Servers sind defekt
- Manche Server weisen mehrere Varianten auf
- Priorisierung DC-Analyse

```
----- GANDCRAB V4 -----
```

```
Attention!
```

```
All your files, documents, photos, databases and other important files are encrypted and have the extension: .KRAB
```

```
The only method of recovering files is to purchase an unique private key. Only we can give you this key and only we can recover your files.
```

## DC-Analyse

- Angriff startete gegen ca. 18:30
- Skript zur Löschung von Kern-Diensten (AD) gefunden
  - DESTRUKTIV
- Malware gefunden
- Anmeldung erfolgte über Terminal-Server mit Benutzer eines Admins Peter Wiśniewsku
- Angreifer war interaktiv tätig

\*) Namen, Daten und Firmen wurden pseudonymisiert

## Auswertung

- Rolle Admin Wiśniewsku ist ungeklärt
  - Ermittlungen offen
  - Admin Wiśniewsku wird aus den Ermittlungen und Tätigkeiten rausgehalten
  
- Neue Ziele:
  - Rolle von Admin Wiśniewsku klären  
(Täter?/Passwort-Komplexität?/Zugangsdaten leaked?)
  - Analyse Terminal Server

\*) Namen, Daten und Firmen wurden pseudonymisiert



# Neue Ereignisse

Von: Patrick Wiśniewski  
An: alle@kunde.de  
Cc:  
Betreff: Fwd: Plik  
Gesendet: 05.04.2019 11:05

Nachricht  Aufstellung Gehälter - Bonuszahlungen - Reisekosten - alle Mitarbeiter - 2012-2018.xls

Dear Sir/ Madam Alle,

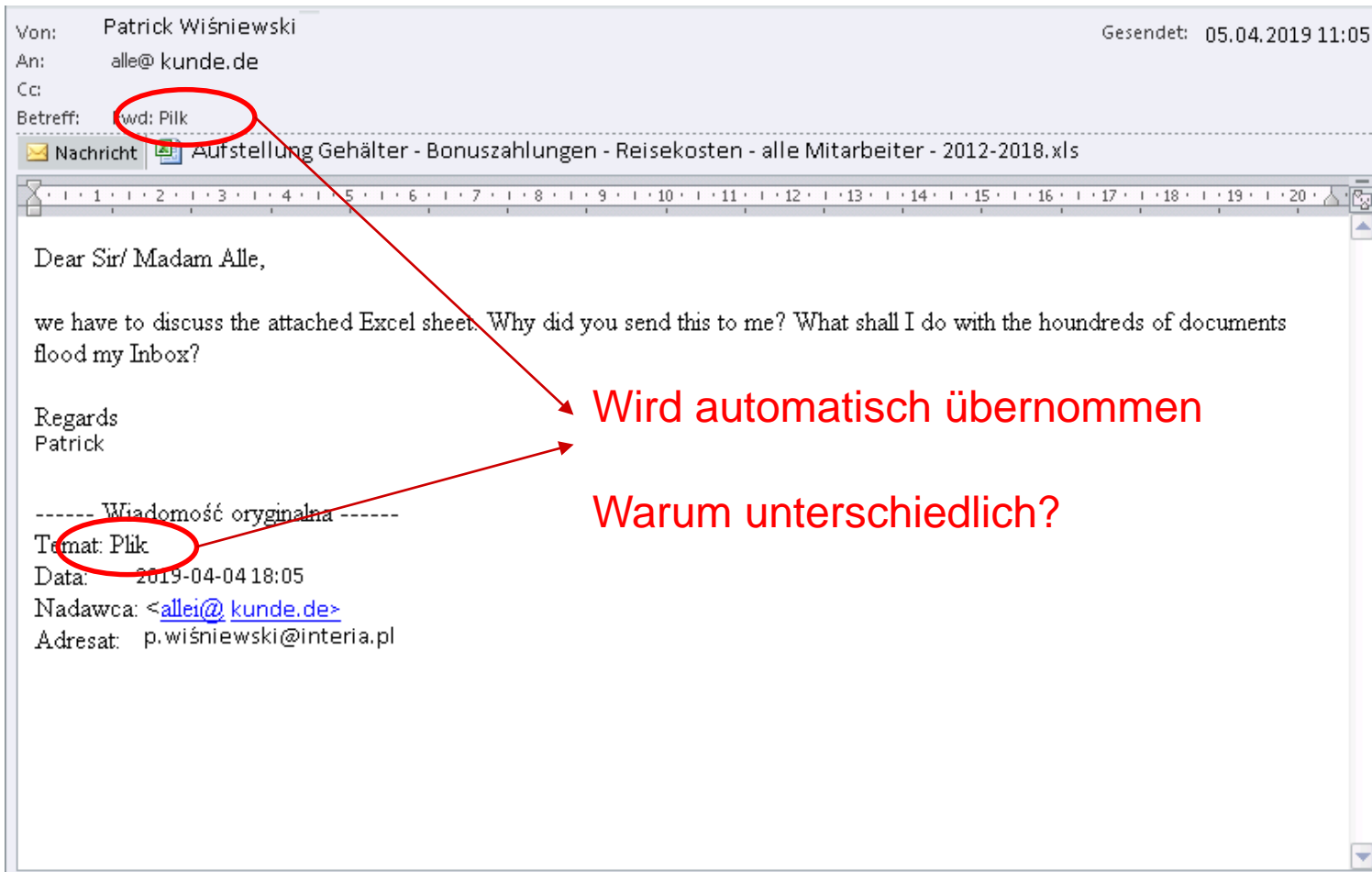
we have to discuss the attached Excel sheet. Why did you send this to me? What shall I do with the houndreds of documents flood my Inbox?

Regards  
Patrick

----- Wiadomość oryginalna -----  
Temat: Plik  
Data: 2019-04-04 18:05  
Nadawca: <[allei@kunde.de](mailto:allei@kunde.de)>  
Adresat: p.wisniewski@interia.pl

\*) Namen, Daten und Firmen wurden pseudonymisiert

# Mail echt?



Von: Patrick Wiśniewski  
An: alle@kunde.de  
Cc:  
Betreff: wd: Plik

Gesendet: 05.04.2019 11:05

Nachrichte: Aufstellung Gehälter - Bonuszahlungen - Reisekosten - alle Mitarbeiter - 2012-2018.xls

Dear Sir/ Madam Alle,

we have to discuss the attached Excel sheet. Why did you send this to me? What shall I do with the houndreds of documents flood my Inbox?

Regards  
Patrick

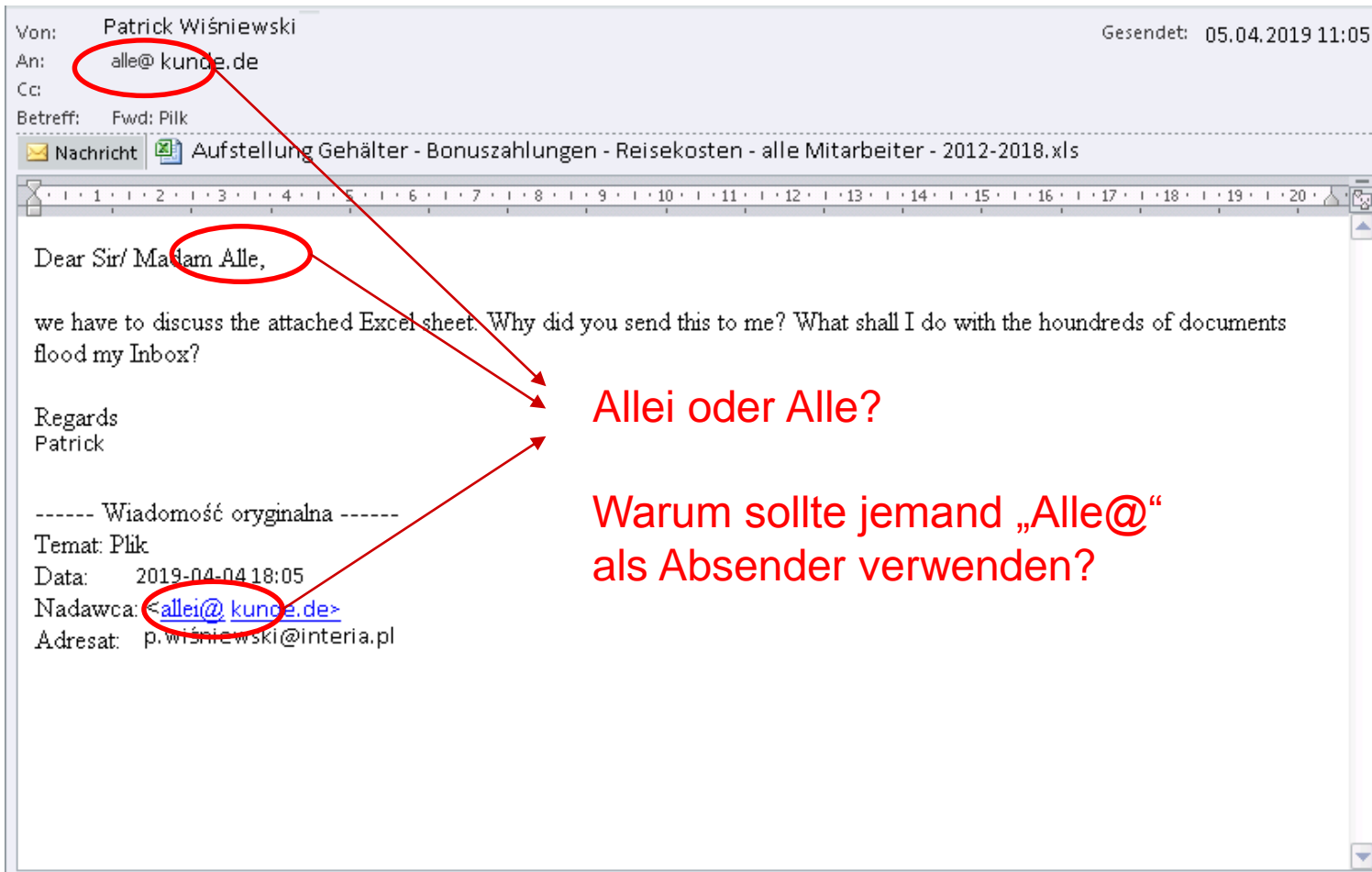
----- Wiadomość oryginalna -----  
Temat: Plik  
Data: 2019-04-04 18:05  
Nadawca: <allei@kunde.de>  
Adresat: p.wisniewski@interia.pl

Wird automatisch übernommen

Warum unterschiedlich?

\*) Namen, Daten und Firmen wurden pseudonymisiert

# Mail echt?



Von: Patrick Wiśniewski  
An: alle@kunde.de  
Cc:  
Betreff: Fwd: Plik

Gesendet: 05.04.2019 11:05

Nachrichte: Aufstellung Gehälter - Bonuszahlungen - Reisekosten - alle Mitarbeiter - 2012-2018.xls

Dear Sir/ Madam Alle,

we have to discuss the attached Excel sheet. Why did you send this to me? What shall I do with the houndreds of documents flood my Inbox?

Regards  
Patrick

----- Wiadomość oryginalna -----  
Temat: Plik  
Data: 2019-04-04 18:05  
Nadawca: <allei@kunde.de>  
Adresat: p.wisniewski@interia.pl

Allei oder Alle?

Warum sollte jemand „Alle@“ als Absender verwenden?

\*) Namen, Daten und Firmen wurden pseudonymisiert

# Mail echt?

Von: Patrick Wiśniewski Gesendet: 05.04.2019 11:05  
An: alle@kunde.de  
Cc:  
Betreff: Fwd: Plik

Nachrichte | Aufstellung Gehälter - Bonuszahlungen - Reisekosten - alle Mitarbeiter - 2012-2018.xls

Dear Sir/ Madam Alle,

we have to discuss the attached Excel sheet. Why did you send this to me? What shall I do with the houndreds of documents flood my Inbox?

Regards  
Patrick

----- Wiadomość oryginalna -----  
Temat: Plik  
Data: 2019-04-04 18:05  
Nadawca: <allei@kunde.de>  
Adresat: p.wiśniewski@interia.pl

Od:  
Do:  
Wysłane: 18:05 Środa 2019-04-04  
Temat: Plik

**Übersetzung von Sender, Empfänger,**

**Datum entspricht nicht interia.pl**  
**Datumsformat ist bei interia.pl anders**

\*) Namen, Daten und Firmen wurden pseudonymisiert

## Passwort

- Intern gab es Passwort-Listen und Skripte mit Username und Passwort (auch genutzter Account Admin Wiśniewsku)
  - Teilweise auch Zugriff für Benutzer
- Eine Passwort-Liste war auch in einem öffentlichen Cloud-Storage ohne Passwort verfügbar (allerdings laut Log keine unbefugten Zugriffe)
- Admins waren die Listen bekannt

\*) Namen, Daten und Firmen wurden pseudonymisiert

## Hypothesen

- Mail enthält viele Widersprüche
- Versandt der Mail an Alle
  - Verteiler „Alle“ war bekannt. Dienstleister war vor Monaten beauftragt worden, diesen abzuschalten
- Inhalt: Gehaltsdaten/Boni sollen Unfrieden stiften
- Verdacht soll vermutlich auf Admin Wiśniewsku gelenkt werden

\*) Namen, Daten und Firmen wurden pseudonymisiert

# Neues Ereignis

**Von:** max.mustermann123@gmx.de  
**Gesendet:** Donnerstag, 06. April 2019 07:25  
**Betreff:** Gehaltsliste aller Mitarbeiter

Hallo zusammen,  
macht euch das nicht stutzig, dass das Arsch von Chef eine Email löschen lässt und das eine Mail von Patrick Wiśniewski überall gelöscht wird? Eine Mail eines polnischen Emailkontos, das nur einen Buchstaben von unserem eigenen tollen Netzwerkadministrator entfernt ist und eine Excel- Gehaltsliste der ganzen Firma mit Bonuszahlungen im Anhang hat?

Von Allen der Mitarbeitern sind dort die Gehälter eingetragen, sogar inkl. Bonuszahlungen. Ich bin verärgert was einige für eine Unmenge an Kohle bekommen und wie die, die die wirkliche Arbeit machen und unter den miesen Strukturen zu leiden haben, abgespeist werden.

Ich habe euch die Liste mal hier zum Wundern und Staunen abgelegt, ist unkritischh zu öffnen da Sie nur im Browser angezeigt wird.

Was ist denn hier los? Mehrfach müssen wir Daten wieder aufwändig neu erstellen weil monatelange Arbeiten einfach gelöscht sind und es keine Rücksicherungen gibt, Mailserver funktionieren wochenlang nicht und es fehlen laufend irgendwelche Server. Jetzt wissen fremde Menschen auch noch darüber Bescheid, was wir hier verdienen- oder nicht verdienen. Sicherheit und Datenschutz scheint es hier nicht zu geben. Das ist mir noch nirgendwo vorher passiert.

[https://www.dropbox.com/s/asdnfcowdvnwf/Geh%C3%](https://www.dropbox.com/s/asdnfcowdvnwf/Geh%C3%9C)

Diese Mail habe ich von einem anderen Konto geschickt, manche im Haus werden nicht glücklich sein.

\*) Namen, Daten und Firmen wurden pseudonymisiert

## Neues Ereignis - Gesichtspunkte

- Abfällige Schreibweise (Arsch von Chef)
- Behauptet Mitarbeiter zu sein
- Nochmalige Übermittlung der „Datei“
- Unmut über „Gehälter“  
(Hilfestellung um Unmut zu schüren)
- Inkompetenz klarstellen
- Hinweis auf Ähnlichkeit zu „Admin“

### Überlegungen:

- Unfrieden stiften?
- Ablenkung vom Täter ?
- Admin als Sündenbock?
- Trittbrettfahrer ?



## Auswertung Terminal-Server

- Wiederherstellung von Daten und Strukturen teilweise möglich
  - Ereignislogs
    - Anmeldung Admin Wiśniewsku auf Terminalserver erfolgte über das Internet (von IP aus dem Ausland)
    - Weitere Anmeldungen von der IP und lokalem DSL Anschluss mit Admin Wiśniewsku und Admin-Kunde
  - gelöschte Ordner:
    - diverse Batch-Files und ausführbare Dateien, darunter auch die bereits auf dem DC identifizierten Dateien
    - Repartitionierungs- und Formatierungsskript
    - Letztes Änderungsdatum 8 Tage vor Angriff

\*) Namen, Daten und Firmen wurden pseudonymisiert

## Auswertung IP-Adressen

- Ausländische IP gehört dortiger Niederlassung eines Musikinstrumentenhersteller
- Regelmäßige Zugriffe von Angreifer-IPs auf Postfächer (Admin/GF) bis Analysezeitpunkt
- IT-Ansprechpartner ist ein externer Service-Dienstleister aus Deutschland
  - Gleicher Anbieter, von dem sich der Kunde aktuell trennt.
  - Weitere Indizien belasten den Geschäftsführer des IT-Dienstleisters
  - Hinweise sind ausreichend für einen Durchsuchungsbeschluss



Angreifer  
lesen  
mit

## Wiederanlauf

- Fast alle Daten konnten wiederhergestellt werden
  - Einige Hindernisse:
    - Große Datenmengen
    - Zugriffsgeschwindigkeiten der alten NAS-Lösung
    - Langsame Netzwerkverbindungen
    - Fehlende technische Ansprechpartner
    - Spurensicherung kostete Zeit
  - Längerer Ausfall eines der Kernsysteme
    - Teilweise sehr aufwendige Verfahren
      - Manuelle Wiederherstellung Raids
      - Zerstörte Backup-Systeme / Kataloge
      - Dateisystem rekonstruieren

## Zusammenfassung

- Schwerwiegender Sabotagefall
  - Ausführungszeit: ca. 4 Stunden (eher lang)
  - Begünstigt durch schlechte IT-Sicherheit und Insiderkenntnisse des Angreifers
  - Ziel: Schädigung des Unternehmens
  - Sabotage - getarnt als Trojaner Angriff
  - Verdacht sollte auf Administrator gelenkt werden
  - Hauptverdächtiger: IT-Dienstleister
  - Großteil der Daten konnte wiederhergestellt werden
  - Trotzdem große Ausfälle

Das war´s...



**Vielen Dank für Ihre Aufmerksamkeit!**

Wolfgang Straßer  
wolfgang.strasser@add-yet.de