@-yet GmbH
Wolfgang Straßer
Geschäftsführer
Dipl.-Kfm.

Cyber Crime: Fiktion oder Wirklichkeit? Erzählungen aus der IT-forensischen Praxis

Firmenportrait

- Juni 2002 gegründet
- inhabergeführt
- Sitz: Leichlingen/Rheinland

- Beratungsschwerpunkte:
  - IT-Risikomanagement
  - IT-Outsourcing und Cloud
  - Informationssicherheit

- @-yet IT Security Akademie

- Zielgruppe:
  - mittelständische und große Organisationen

IT-RESULTING IM FOKUS

IT Risikomanagement

- Bewusster Umgang mit den Risiken, die sich für Unternehmen und Organisationen durch den Einsatz von IT ergeben können.

IT Risikomanagement

Betrachtung der IT aus dem Blickwinkel
Risiken für das Geschäft durch unzureichende:

Verfügbarkeit	⇒	Business Continuity
Sicherheit	⇒	Business Security
Regelwerke	⇒	Business Compliance

IT-RESULTING IM FOKUS

IT Risikomanagement

Zentrale Fragestellungen:

- welche Geschäftsprozesse
- welche Fertigungsprozesse
- welche Daten

sind für den Unternehmenserfolg besonders wichtig

und

wie groß ist die Abhängigkeit dieser Prozesse von der IT und den begleitenden Prozessen?

- Welche gesetzlichen Auflagen gibt es?
- Welche vertraglichen Vereinbarungen?

@-yet Bausteine IT Risikomanagement

Business und IT Security

Business Continuity

Compliance Datenschutz

Incidence Response IT-Forensik

IT-RESULTING IM FOKUS

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.

Zentraler Baustein von IT-Risikomanagement:

- Business Security

Business Security: was ist das?

Business Security oder IT Securizty
ist kein Selbstzweck!

Business Security schützt

Geschäft, Geld und Management

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!

IT-RESULTING IM FOKUS

Warum Business Security?

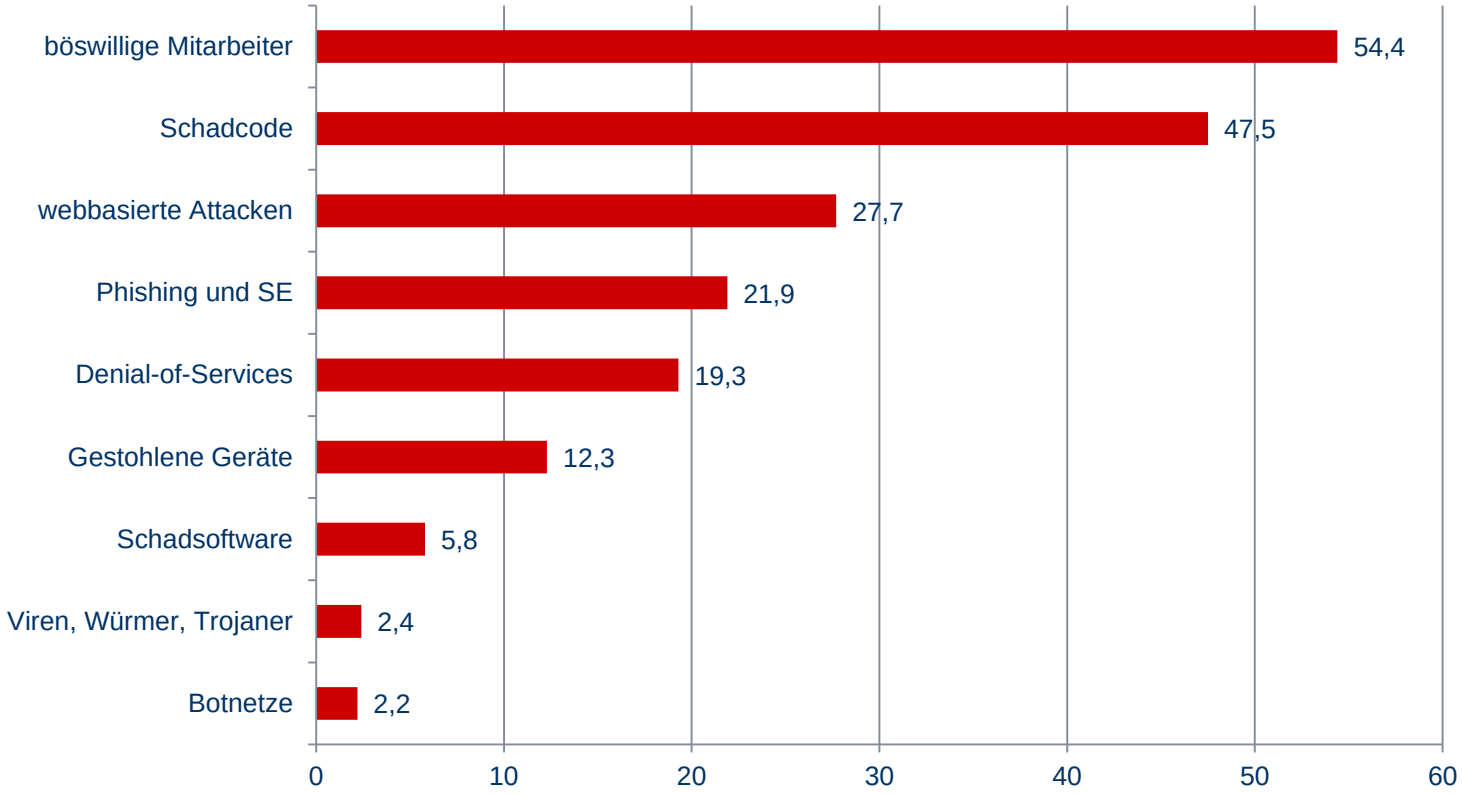
- Die deutsche Wirtschaft im Fokus der Attacken
  - Deutschland ist die Exportnation Nummer 1 oder 2
  - Deutsches Ingenieurwissen ist führend

Einige Fakten zum Thema IT-Sicherheit

- **CyberCrime Umsatz übertrifft den Drogenhandel**

Einige Fakten zum Thema IT-Sicherheit

Durchschnittliche Zeit in Tagen, die zur Abwehr von Angriffen benötigt wird



Ponemon Studie 2015

IT-RESULTING IM FOKUS

- Wer greift an und warum?

Wer greift an?

- Staaten
- Wettbewerber
- organisierte Kriminalität
- befürchtet: Terroristen
- sonstige

Motive der Angreifer

- vor allem wirtschaftliche
  - Wirtschaftsspionage/Konkurrenzausspähung
  - Erpressung: Bsp. Locky
  - Geld: Bsp. CEO Fraud
- Rache
- ethische Motive
- „Spaß am Hacken“
- „beleidigt“ sein
- und vieles Unvorstellbares mehr

- Wie wird angegriffen?

Wie wird angegriffen?

- Informationsbeschaffung von innen oder SocialNetwork
  - Ausnutzen physischer und organisatorischer Schwachstellen
  - Social Engineering
- Datenträgerklau oder - angriff
  - Smartphones, Pads, Notebooks etc.
- Hackingangriff von außen
- **immer mehr über manipulierte**
  - Websites, Portale, Onlineshop etc.
  - Cloud
  - APPS und Mobiles

IT-RESULTING IM FOKUS

- Beispiel 1

Beispiel 1

- Der Auftrag:
  - Überprüfung der neuen Unternehmenszentrale auf
    - Zugangssicherheit
    - Awareness von
      - Management
      - Mitarbeitern
      - Externen Dienstleistern
    - Sicherheit der Netzzugänge, falls Zutritt gelingt
    - WLAN Sicherheit
      - Check von draußen
    - Endgerätesicherheit

Beispiel 1

- Der Auftraggeber:
  - Typisches mittelständisches Unternehmen
    - innovativ
    - weltweit präsent
    - ökonomisch erfolgreich
    - inhabergeführt

Beispiel 1

- Der Ablauf:
  - Internetrecherche über
    - Gebäudestruktur (GoogleEarth)
    - Mitarbeiter (wer macht was)
      - Eigene Webseiten
      - SocialNetwork (XING, Linkedin)
  - Gebäudebeobachtung
    - Wann kommen und gehen
      - Mitarbeiter
      - Putzdienste
      - Wachdienst
  - WLAN Aufnahme
  - „Angriff“

Beispiel 1

- Der Angriff mit 2 Teams je 2 Personen
  - Frontdesk/Empfang
    - Erfolglos - sehr gut trainiert, sehr höflich, aber bestimmt
  - Tiefgarage
    - erfolgreich
    - Mitarbeiter waren sehr bemüht uns zu helfen..

Beispiel 1

- Ablauf tagsüber im Gebäude (3 zügig)
  - trotz Zugangssicherung mittels SmartCard
    - Gebäude
    - Etagen
    - Büros
    - Aufzüge

    - waren wir überall und stundenlang

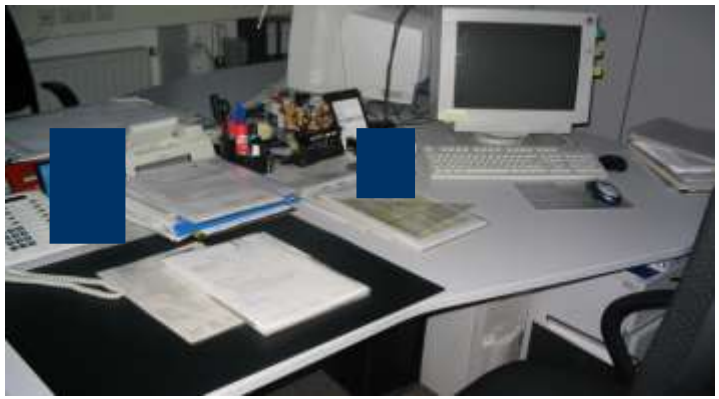
  - Installation von WLAN-Routern in allen 3 Gebäuden

  - Zugang zu Arbeitsplatzrechnern
    - Installation von MalWare mittels USB Stick
      - an ca. 50 AP´s
      - in allen Gebäuden und Etagen

Beispiel Social Engineering

Offizieller Zutritt als Besuche

- Nutzung interner Ressour
- „Dumpster Diving“
- Diebstahl von materiellen und imm enständen



Beispiel Social Engineering

- Diebstahl von Daten auf USB-Stick
- Installation von Keyloggern
- Installation eines Wireless-Access-P
- Sabotage von kritischen Systemen

Beispiel: Infrastruktur Assessment

- außenstehende / Besucher können Gebäude & Räume „ungehindert“ betreten
- Firmeninterne Unterlagen einfach zugänglich
- Verteilerschränke sind nicht abgesperrt
- vertrauliche Daten in den Büros werden nicht weggesperrt bzw. Büros nicht abgeschlossen

Beispiel 1

- Ablauf abends am und im Gebäude
  - Versuch von außen auf die WLAN AccessPoints zuzugreifen
    - WLAN 1: erfolgreich ins Schulungsnetz gekommen
    - WLAN 2: schlecht positioniert, zu weit von der Straße weg
    - WLAN 3: hervorragender Empfang, leider Wackelkontakt
  - Putzkolonne „angegriffen“
    - Leiterin extrem hartnäckig
    - hat alle AP´s (Chef, Firmenfacilitymanager) versucht zu erreichen – erfolglos
    - sie hat uns dann zum defekten WLAn gebracht!!
      - dort saß jemand….
    - WLAN Router erfolgreich ausgetauscht

Beispiel 1

- Ablauf spätabends und nachts
  - Versuch von außen auf WLAN 3 zuzugreifen
    - Vollzugriff und -zugang zum Unternehmensnetz
    - Innerhalb von 3-4 Stunden erste Adminrechte
    - mehrere hundert Passwörter geknackt
      - Viel zu kurz und leicht
    - im Laufe der Nacht: System- und Applikationsrechte
    - Wir hätten unbemerkt Daten abziehen/manipulieren/löschen können
- Ablauf Tag 3
  - Notebook und Smartphonechecks
    - Leichter Zugriff auf alles, da
      - keine Verschlüsselung
      - zu schwache Pins und Passwörter

- Rückschlüsse Beispiel 1

Rückschlüsse Beispiel 1

- Ohne Awareness bei Management und Belegschaft
  - hoher technischer Gebäudeschutz wirkungslos
  - extrem leichter Zugang zu Endgeräten
  - nicht ausreichende Passwörter

- War man einmal im Gebäude, war alles möglich
  - kein Netzzugangsschutz
  - Fremdgeräte wurden nicht erkannt
    - WLAN Access Router
    - Notebooks

Maßnahmen Beispiel 1

- Awarenessschulungen für alle
  - Umgang mit Fremden
  - keine Unbekannten an das eigene System lassen
  - fremde Datenträger nicht ungeprüft verwenden
    - USB
    - CD etc.
  - das „richtige" Passwort verwenden

- Technische Maßnahmen
  - USB Blocker
  - Netzsegmentierung
  - Netzzugangssperre für Fremdgeräte
  - Lange und komplexe PW fordern/erzwingen
  - Festplattenverschlüsselung Notebooks

- Beispiel 2

Beispiel 2

- Der Auftrag:
  - Forensik eines Angriffs
- Der Auftraggeber
  - DAX Konzern

Beispiel 2

- Was war passiert?
  - gezieltes Spearphishing auf
    - Vorstände und deren Assistentinnen
    - IT-Admins
  - wochenlanger Vollzugriff auf das Unternehmen konnte nachgewiesen werden
  - die Malware konnte auf hunderten Arbeitsplätzen und Servern nachgewiesen werden
    - Analog zu Bundestag hatte der Angreifer die zentralen Serverdienste im Zugriff – Golden Ticket

Beispiel 2

- Wie konnte das passieren?
  - Die anzugreifenden Personen waren offensichtlich bekannt
    - Websites
    - Socialnetworks??
  - Die Rechner und user hatten alle Adminrechte
  - Kaum Netztrennung –
    - ist man einmal drin, kommt man überall hin

- Rückschlüsse Beispiel 2

Rückschlüsse Beispiel 2

- Auch hier
  - Mangelnde Awareness bei Management und Belegschaft
    - speziell IT-Admins!!!!
- Virenscanner und Spamfilter sind wirkungslos bei firmenspezifischen Attacken
  - nicht auf Technik verlassen
  - Emails von unbekannten Absendern
    - löschen oder
    - von IT untersuchen lassen
  - Wachsamkeit ist immer notwendig

empfohlene Maßnahmen Beispiel 2

- Umgang schulen mit
  - fremden emails
  - unbekannten Webseiten
    - können extrem gefährlich sein
    - auch und gerade Werbebanner
  - mit Socialnetwork
    - gar einschränken??
      - der Exhibitionismus ist sehr stark
- keine Adminrechte auf Endgeräten
- bei IT-Admins
  - Trennung von Adminaccount und „Normaluseraccount“

IT-RESULTING IM FOKUS

- Beispiel 3

Beispiel 3

- Der Auftrag:
  - Forensik eines Angriffs
- Der Auftraggeber
  - N.N.
- Was war passiert?

Beispiel 3

- strengvertrauliche Unternehmensinformationen tauchten im WEB auf
  - Unternehmenstrategieen
  - finanzielle Informationen
  - „Lobbyarbeit“
- eindeutige Rückverfolgbarkeit auf ein Aufsichtsratsmitglied

Beispiel 3

- Analyse ergab
  - Emails mit vertraulichen Infos und Anhängen wurden aus dem Vorstandsbüro auf den Privataccount geschickt
  - der Privataccount war gehackt
  - Kennung und PW wurden in Klarschrift in einem Bikershop gefunden
    - es war bekannt, daß der AR bekennender Biker ist…
  - PW extrem schwach – 5 stellig

- weitere Analysen beim „Opfer" ergaben
  - ein PW für nahezu alle Anmeldeszenarien
    - Firma
    - Shops
    - sonstige Portale

- Rückschlüsse Beispiel 3

Rückschlüsse/Maßnahmen Beispiel 3

- Firmenemails auf Privataccounts unterbinden
  - schon gar nicht in Firmenverteilern aufnehmen
- ein PW für alles ist keine gute Idee
- sich nicht vorbehaltlos auf die Sicherheit von
  - Onlineshops
  - Webseiten verlassen

- Beispiel 4

Beispiel 4

- Der Auftrag:
  - Forensik eines Angriffs
- Der Auftraggeber
  - mittelständisches Unternehmen der Nahrungsmittelbranche
- Was war passiert?

Beispiel 4

- Was war passiert?
  - Virenausbruch in der Produktion
    - Locky!!
  - tagelanger Produktionsausfall
    - und das bei 7x24 Stunden Produktion
    - täglicher Umsatzverlust: 200 T€
    - Keine Chance den Produktionsausfall wieder „reinzuholen“
    - Pönalen drohen zusätzlich, da feste Lieferzusagen

Beispiel 4

- Wie konnte das passieren?
  - Virus wurde durch email eingefangen
  - aus Performancegründen ist es dort in der Produktion nicht möglich einen Virenscanner einzusetzen – ist häufig so
  - der infizierte Rechner hatte
  - allerdings einen Zugang zum Internet und
  - der user Adminrechte
  - keine Netzsegmentierung
    - deshalb Flächenbrand und totaler Produktionsausfall

- Rückschlüsse Beispiel 4

- abschließend

- Online Banking
- Mobile Payment

- Online Banking
  - HBCI kann derzeit als einziges sicheres Verfahren gelten
  - Bei allen anderen Verfahren liegen Schadensfälle vor

- Mobile Payment
  - Endgeräte sind grundsätzlich unsicher
  - Nutzung freier WLAN´s ist grundsätzlich problemtisch
    - Sie wissen nie so ganz genau, wer der Owner ist
  - Payment APPS
    - mehrere geprüft
      - keine war wirklich gut
      - manche haarsträubend schlecht

- Mobile Payment
  - Sicherheit mit Biometrie?
    - Sie haben 10 Finger und 2 Augen und das wars
  - NFC?
    - Taschendiebstahl für Gichtkranke einfach gemacht

- Was tun?

Ganzheitliche Betrachtung Business Security

Physische Sicherheit

Gebäude- und Zugangsschutz

Geräteschutz

Informations-Sicherheit

State-of-the-Art Security Produkte & Technologien

Organisatorische Sicherheit

Security Policies, Prozesse,

System- und Gerätemanagemnt
Mitarbeiter+Management Awareness

IT-RESULTING FOCUS

Vorgehensweise

Bestimmen Sie Ihren **Schutzbedarf und IHR Risiko**

- Welche Daten sind für ein Unternehmen wie wichtig?
  - Datenklassifikation, ISMS
  - Wer darf auf welche Daten zugreifen und wer entscheidet das?
- Welche Prozesse sind wie wichtig?
  - Business Impact Analyse
  - Ab wann verliert ein Unternehmen wieviel Umsatz, wenn Prozesse stehenbleiben?
- Welche gesetzlichen Mindestauflagen müssen erfüllt sein.
  - z.B. Datenschutz/BDSG
  - IT-Sicherheitsgesetz

Vorgehensweise

Statusfeststellung und Risikobewertung: wo stehen Sie?

- Status organisatorische Sicherheit
  - Policies
  - Awareness

    @-yet tools:
    - Social Engineering/Phishing
    - Policy Check
- Status physische Sicherheit
  - Gebäudeschutz

    @-yet tool:
    - Social Engineering
- Status IT-Sicherheit

  @-yet tools
  - Onsite- und Offsite-Pentests
  - Infrastruktur- und Continuitycheck

IT-RESULTING IM FOKUS

Was wollten wir Ihnen vermitteln

- Security zu vernachlässigen
  - ist fahrlässig
  - kann existentiell werden
- vor der Implementierung von Schutzmechanismen und –maßnahmen
  - **immer erst die Definition der Sicherheitsziele**
- die Technik ist komplex, aber beherrschbarer als vermutet,
- aber ohne Organisation und bewusstes Umgehen mit der IT ist sie wertlos

Erste Schritte

- WLAN Hotspots, deren Betreiber man nicht kennt, meiden
- Lange, möglichst 18-stellige, komplexe PW nutzen
- sicheres Onlinebanking nutzen
  - HBCI
- Alle Festplatten sollten verschlüsselt sein
- Alle Sicherheitspatche der Hersteller umgehend installieren
- Firewall immer auf dem neuesten Stand halten
- Virenscanner und Spamfilter immer aktuell halten
- Vorsicht vor Webseiten und Apps, die man nicht kennt und nicht unbedingt braucht
- Clouds möglichst nur verschlüsselt nutzen
  - Wichtig: nur wenn Sie den Schlüssel selber haben, ist Verschlüsselung zu trauen – wie beim eigenen Haus
- Systeme regelmäßig von Fachleuten checken lassen
- **… und ganz einfach Vorsicht walten lassen**

Ihre Fragen bitte …

Vielen Dank für Ihre Aufmerksamkeit!

Wolfgang Straßer
wolfgang.strasser@add-yet.de