REGIONALES RECHENZENTRUM ERLANGEN [RRZE]

IT-Sicherheit

Digitales Rüstzeug in der IT-Sicherheit am RRZE

Systemausbildung − IT-Dienste des RRZE und der FAU,
16.06.2021, Marcel Ritter, RRZE

FRIEDRICH-ALEXANDER UNIVERSITÄT ERLANGEN-NÜRNBERG

AGENDA

1. Bedrohungsszenarien
2. Angriffe
3. Gegenmaßnahmen
4. Reaktion & Analyse
5. Aktuelles

BEDROHUNGSSZENARIEN

- Zielsetzung der Angreifer
- Verbreitungswege
- Ausprägungen

Welche Ziele verfolgen die „Einbrecher“?

- Zugriff auf
  - Schützenswerte / wertvolle Daten (z.B. Forschungsdaten)
  - Logins / Passwörter (oder Passwort-Hashes), damit Zugriff auf weitere Systeme
- Missbrauch von Ressourcen
  - Spam-Mail
  - (D)DOS-Client, Botnet / Control-Server (Zentral vs. P2P)
  - Rechenleistung (Bitcoin-Mining)
  - Hardware (Drucker, Kamera, …)
  - Scan / Angriff auf weitere Systeme
- Erpressung
  - Datenverschlüsselung! (Ransomware)
  - Aber auch durch Zugriff auf persönliche/vertrauliche Daten

Auf welchem Weg drohen Gefahren?

- Nicht technisch:
  - Diebstahl
  - Social Engineering
  - Entsorgung von „Datenträgern“ (analog wie digital)
    - › Verkauf gebrauchter Speichermedien, Recycling von SSD-Speicherchips in USB-Sticks
- Technisch:
  - Speichermedien mit Schadsoftware
  - Drive-By (Web) / Mail-Attachments
  - Scans / Aktive Angriffe

Wie können technische Gefahren aussehen?

- Hardware:
  - USB-Killer-Sticks (Überspannung)
  - Programmierte USB-Sticks („Rubber Duck“)
- Hard- oder Software:
  - Floppy/USB-Stick/SD-Card mit Schadsoftware
  - Keylogger / Screenlogger
  - Backdoors
- Software
  - Viren, Würmer, TrojanerRootkits
  - Adware / Nagware / Ransomware

OFFENSICHTLICH BIS „UNSICHTBAR“

IT-Sicherheit jenseits vom klassischen Server/PC

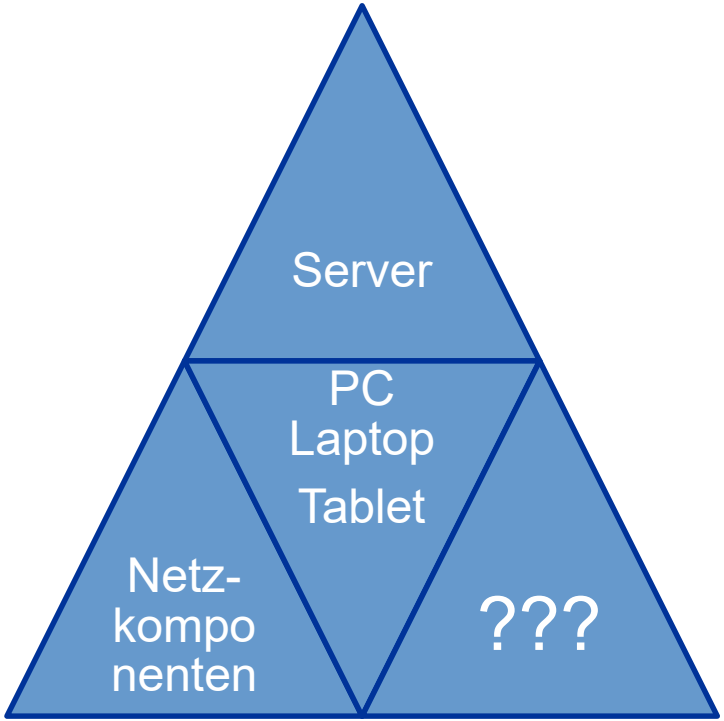
- „unsichtbare“ IT-Geräte (IoT)
- „virtuelle“ IT-Systeme

Altbekannte Gefahrenquellen

- Server
- Endgeräte
- Netzwerkkomponenten

- Aber:
  - Zunehmend nur

    „die Spitze des Eisbergs“



Gefahrenquelle: „Intelligente Hardware“ und „Internet of Things“ …

Klassische IT-Komponenten:

- Netzwerkkomponenten: WLAN-AP, IP-Telefon,…
- Drucker/Kopierer

Mobile Geräte

- Handy, Tablet, Smart-Watch

IoT (Internet of Things), Home Automation

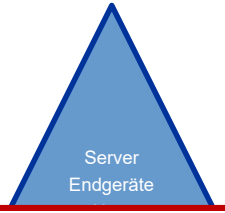
- Industrieanlagen, Auto, Kühlschrank, …

Multimedia-Geräte

- DVD/Blu-ray-Player, Medienstation

Medizingeräte

- Herzschrittmacher, Insulinpumpen, …



Nach einer anfänglichen Hype-Phase gibt es oft **keine Patches** vom Hersteller mehr. Damit werden die Geräte verwundbar!

Besonders „attraktiv“, weil vielseitig:

- Abhören/Mitschneiden von
  - Telefonaten
  - SMS
  - Mails
  - Chats
  - Internetverbindungen
- Medien
  - Bild / Video
  - Ton
  - Position (GPS)
- Und alles: per Fernsteuerung (de-)aktivier- und steuerbar!

Virtualisierung

- Vollvirtualisierung
  - Eigentlich wie „echte“ Server
  - Aber: Aufwand/Kosten wesentlich geringer, deswegen
    - Oft hoffnungslos übertriebene Anzahl von VMs, gefolgt von
    - Mangelhafter Betreuung und daraus resultierendem
    - Sicherheitsrisiko

- Container (wie Vollvirtualisierung, aber zusätzlich…)
  - Update-Strategie: Keine – bei Neustart: Reset oder komplett neues Image
  - Keine automatischen Updates
  - Quellen potentiell unsicher / undurchsichtig

Cloud-Dienste

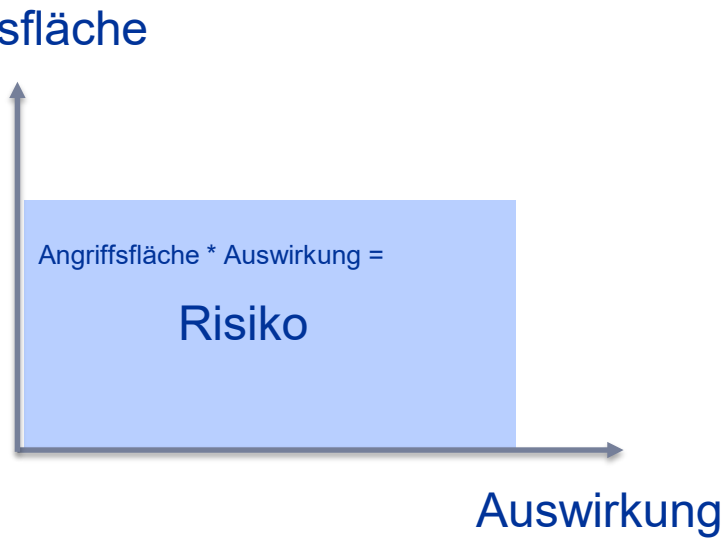
- Vorteile
  - Oft günstige/kostenlose Angebote
  - Komfortable Nutzung
- Nachteile
  - Verarbeitung von Daten/Dokumenten auf Servern Dritter
  - Unterliegen evtl. anderer Jurisdiktion (Behörden-Zugriff)
  - Kleingedrucktes (Rechte an Bildern, etc.)
  - Datenhoheit / Souveränität

GEGENMASSNAHMEN

- Sicherheitsvorfälle verhindern
- Sicherheitsvorfälle erkennen
- Auswirkungen reduzieren

Gegenmaßnahmen - Zielsetzung

- Verminderung „Angriffsfläche“
  - Gepatchte Software (Updates)
  - Nur benötigte Dienste
  - Beschränkung der Zugriffsmöglichkeiten
    - Login/Passwort, lokal (z.B. Subnetz), temporär (z.B. 10/s)
  - Keine Klartext-Authentifizierung (FTP, telnet, rsh, …)
- Verminderung der Auswirkungen
  - Dienste als nichtprivilegierter Benutzer ausführen
  - Ausführung in gesicherter Umgebung (chroot, separate VM)
  - Ressourcenbeschränkung (DOS-Attacken)
  - Role Based Access Control (AppArmor, SELINUX)



Gegenmaßnahmen - physische Sicherheit

- Bei direkten, physischem Zugriff auf Geräte viele Angriffsszenarien einfach möglich, deswegen:

- Beschränkung des direkten Zugriffs
  - Gesicherter Rechnerraum
  - Abgeschlossene Büroräume / Schränke
  - Leicht transportable Geräte sichern (z.B. Kensington-Lock)
  - Absicherung von Netzwerk-Verkabelung

  - Schwieriger bei mobilen Geräten (Laptop, Handy), weil physischer Zugriff leicht möglich
    - Daten-Verschlüsselung
    - PIN-Code / Fingerabdruckscan etc.

Gegenmaßnahmen – technische Sicherheit

Lokaler Rechner

- Updates / Aktuelle OS-Versionen (z.B. Windows 7 nur mit ESU!!!)
- Zugriffsmöglichkeiten/Dienste einschränken
- Virenscanner / Malware-Detection
- Lokale Firewall
- Backup (!)

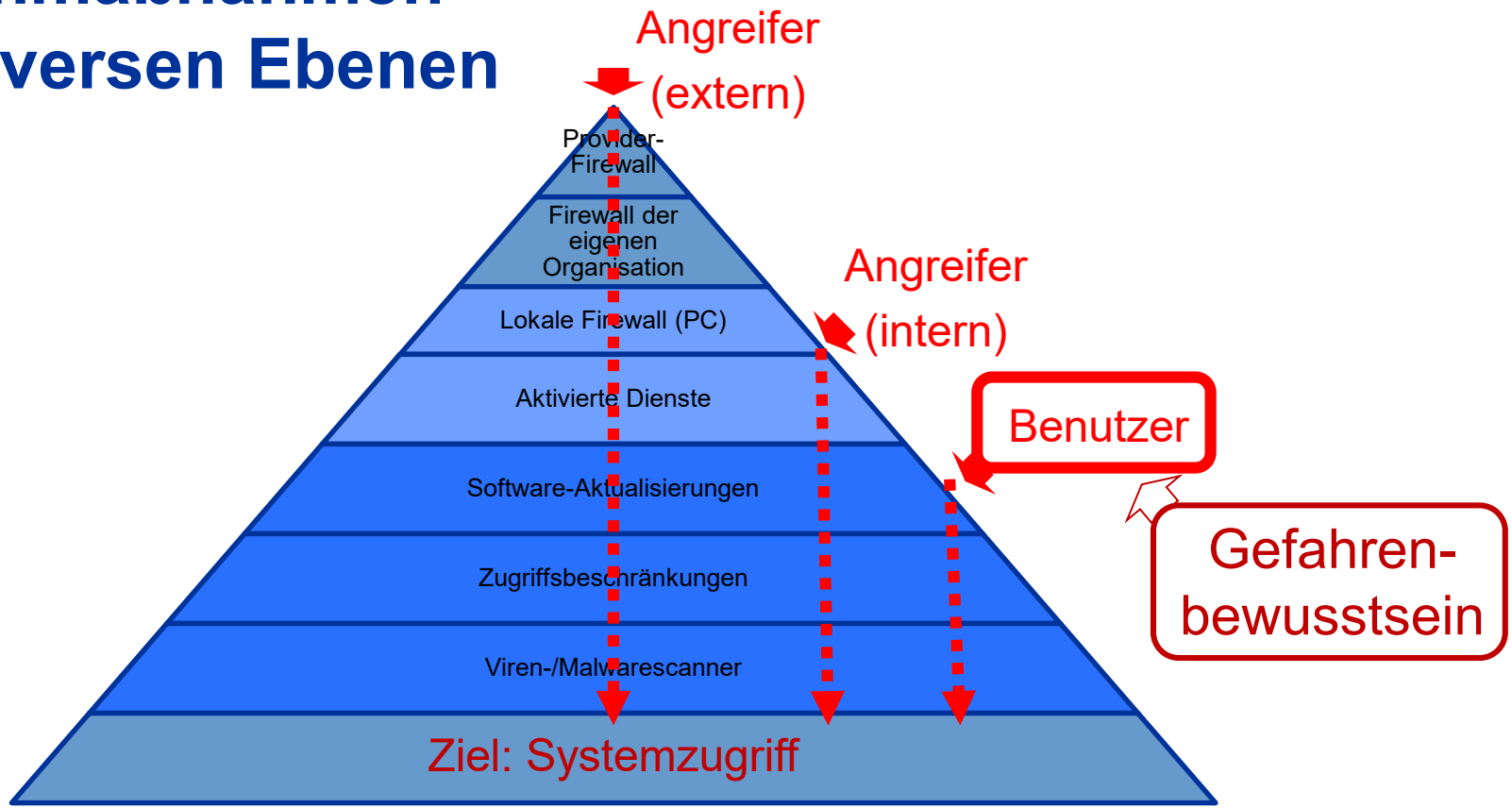
Netzwerk

- Firewall
- Priv. Subnetze (mit Proxy / NAT (Source+Destination) (SSL!))
- Intrusion-Detection/-Prevention (SSL!)

Proaktive Analyse eigener Systeme

- Nessus / OpenVAS (http://sectools.org/vuln-scanners/)

Gegenmaßnahmen auf diversen Ebenen



ANALYSE VON VORFÄLLEN

- Erkennen & erste Schritte
- Analysieren
- Beheben & Vorbeugen

Erkennung von Vorfällen

- Netz-seitig:
  - Verdächtige Netzverbindungen
    - Hohe Anzahl (SPAM)
    - Unbekannte Kommunikationspartner
  - Meldung von außen
- Host-seitig:
  - HIDS (Host Intrusion Detection System)
    - Überwachung von Dateien:
      - Änderungen (Checksummen, Zeitstempel)
      - Ungewöhnliche Dateien (core – oft Nebenprodukt!)
    - Überwachung von Prozessen
    - Überwachung von Netzverbindungen

Erste Schritte bei Vorfall

- Mögliche Reaktionen
  - Stromstecker ziehen
  - Netzwerkstecker ziehen
  - Laufen lassen und weiteres Verhalten beobachten
- Andere Systeme durch Vorfall potentiell gefährdet oder Hilfe gewünscht?
  - Meldung an abuse@fau.de
  - Gerne auch Meldung zur reinen Information
- Ermittlungsbehörden involviert?
  - Angeforderte Daten sichern, Herausgabe aber
  - Nach Prüfung der Anfrage durch Datenschutzbeauftragten
  - Durch den Datenschutzbeauftragten
  - Rechtliche Absicherung!

Analyse von Vorfällen

- Prinzipiell gilt:
  - Analyse einfacher, je vollständiger die Informationen
- Sicherung der zur Verfügung stehenden Daten
  - Log-Files (z.B. Protokoll der Zugriffe / Logins)
  - Sicherung des Dateisystems (oder Teilen davon)
  - Sicherung der Datenträger (Unterschied zu Dateisystem?)
  - Speicher-Dump
    - › Prozessliste, geöffnete Dateien, aktive Netzverbindungen
- Bei Analyse am laufenden System: **VORSICHT!**
  - … erfordert Login (Passwort!)
  - … benötigt entsprechende Tools

Analyse von Vorfällen

- Alles gesichert, aber trotzdem gehackt? Welche Fragen sollte ich stellen?
  - Auf welchem Weg wurde ich gehackt?
  - Warum war der Angriff erfolgreich?
  - Welche Auswirkungen hat der Vorfall für das übrige IT-Umfeld?
- Welche Schlüsse kann ich ziehen? Wie kann ich dem zukünftig vorbeugen?
  - Welche Gegenmaßnahmen sind möglich (und verhältnismäßig)?

AKTUELLES

- Entwicklungen und Beispiele

Phishing – gut gemacht: Bewerbung (12/2016)

Do 08.12.2016 02:23

Andreas M <a.m@s.com>

Bewerbung als Studentische Hilfskraft

An Ritter, Marcel (RRZE)

Nachricht | Bewerbung von Drescher.xls (2 MB) | Bewerbung von Drescher.pdf (135 KB)

Sehr geehrte Damen und Herren,

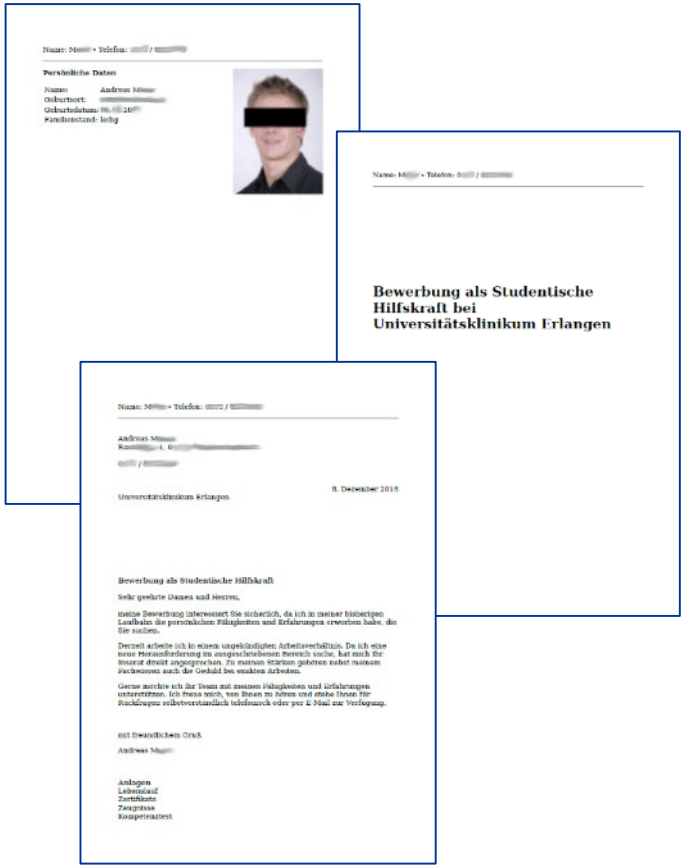
hiermit bewerbe ich mich bei Ihnen für die die Stelle als Studentische Hilfskraft. Meine vollständigen Bewerbungsunterlagen können Sie dem Anhang entnehmen.

Ich freue mich auf Ihre Rückmeldung und stehe Ihnen bei Rückfragen jederzeit gerne zur Verfügung.

Mit freundlichem Gruß

Andreas M

Anlagen
Lebenslauf
Zertifikate
Zeugnisse
Kompetenztest



Social Engineering – auf hohem Niveau

Bewerbung per Mail

- Saubere Sprache
- Korrekte Ansprache der Personalstelle
- Korrekte Referenz auf tatsächlich ausgeschriebene Stelle
- Angehängter Lebenslauf (PDF)
- Angehängtes **Excel** (?) mit Bewerbung

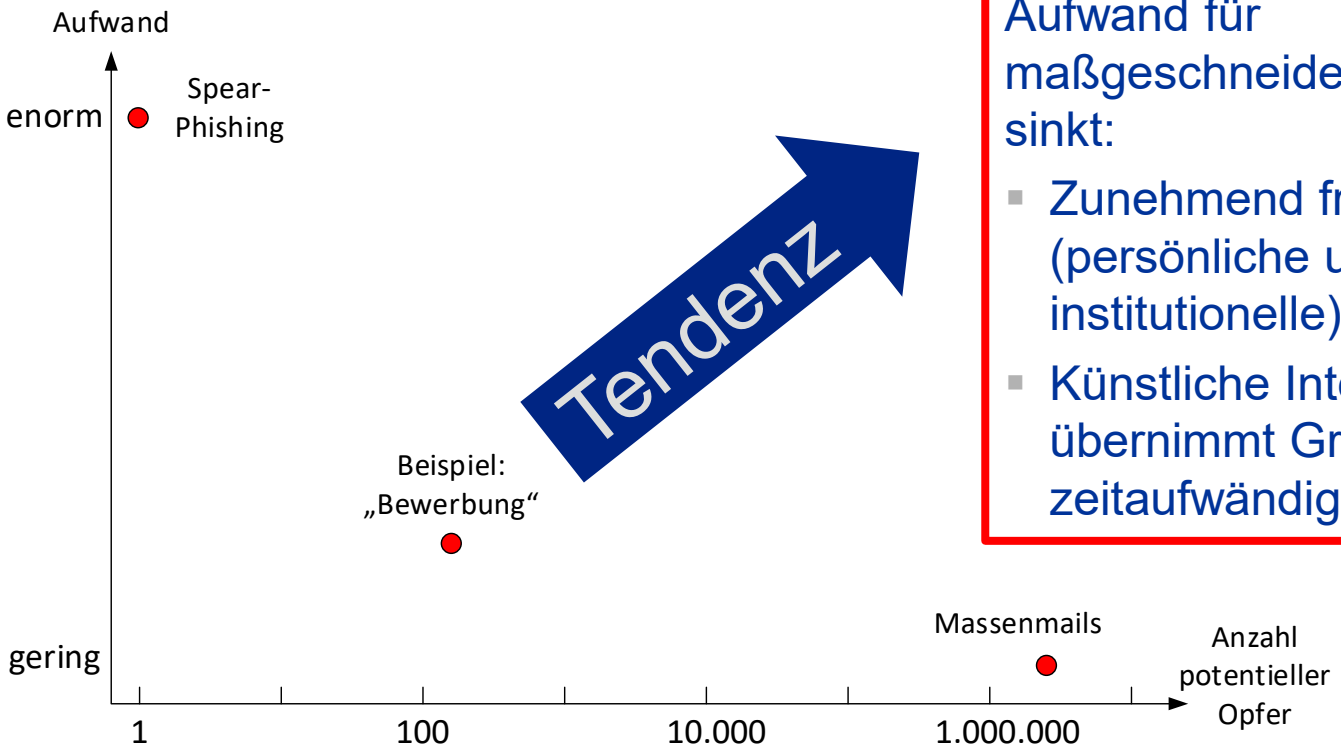
Schadfunktion

- Crypto-Trojaner
- Aktiviert durch Excel-Makro

Quelle der Daten

- Datenbank von Arbeitsvermittlern

Aufwand / Nutzen & Erwartete Entwicklung



Aufwand für maßgeschneiderte Angriffe sinkt:

- Zunehmend frei verfügbare (persönliche und institutionelle) Informationen
- Künstliche Intelligenz übernimmt Großteil der zeitaufwändigen Arbeit

2021:

Es geht auch ganz klassisch … ohne jegliche (künstliche) Intelligenz …

Schlecht gemacht, trotzdem (mehrfach!) erfolgreich…

Hello,

I need you to run a quick task for me. Please send me an email as soon as possible.

Regards,
Prof. Dr. *Max Mustermann*
Chair for *Scientific Stuff*

Dear Max,

Yes I am available.

Regards,

Erika

Dear Erika,

thank you for getting back to me. I need your assistance to get some Gift cards from any store around now. There are some prospects I need to send Gift Cards today but I can't do that right now because I’m currently busy in a meeting so I can't handle things at my end here. Let me know if it 's possible to get them right now, so I can tell you which products I would need and what amount.

I‘ll reimburse you.

Dear Max,

I can get them but I am not sure where to get them from as I haven't gone to too many stores here apart from the supermarket and Vodafone store.

Dear Erika,

you can get the gift cards from Kaufland, Aldi, REWE-Supermarkt nearby. I need 6 Google play gift cards with €200 on each card from the store. When purchased, Kindly scratch off the cards PIN panel to reveal the code and take a picture of the cards and send them to me on here and keep the physical cards a receipt for reference purpose. Please get back to me real soon if you can get this done.

Thanks

Rewe is nearby. So, I need ask for google play gift cards and after purchasing do as you instructed?

Yes, exactly. I will be waiting to hear from you soon.

Thank you.

I sent you an email with the picture of the card. Can you please confirm that this is what you need?

Yes, that's correct. Go ahead with the purchase.

Yes ok thanks.

Dear Erika, I'm still waiting to hear from you. Were you able to purchase the gift cards? Please keep me posted.

Yes I have purchased them for 200 euros each. Just scratching off the pin panel in order to get a picture of codes which I shall send you soon.

Please find the pins of the gift cards attached. Let me know if these are fine.

Got them, thanks! I will mail you back as soon as I get acknowledgement about the card‘s confirmation from the prospect. Kindly keep close to your mail.

Yes sure.

Dear Erika, are you still around the store?

No. I’m at home right now.

Dear Erika, all the cards are confirmed okay. Thanks so much for your time and kindness. But I would like you to get 14 more cards …

Okay, thanks. I really appreciate your kindness. Kindly send your account details along with the cards in the morning for the reimbursement.

Yes sure no. Kindly be available over mail in te morning in case I need to ask something related to the purchase.

Okay no problem. Good night.

Good night.

Good morning Erika, how are you? I hope this email finds you well. Thanks for yesterday‘s task, I really appreciate it. I would like to know when I should be expecting the remaining cards you promised to get this morning. Get back to me as soon as possible.

I shall be going to the supermarket soon to get the cards. Shall let you know once I get them.

Got the cards. Shall be sending you the pictures soon.

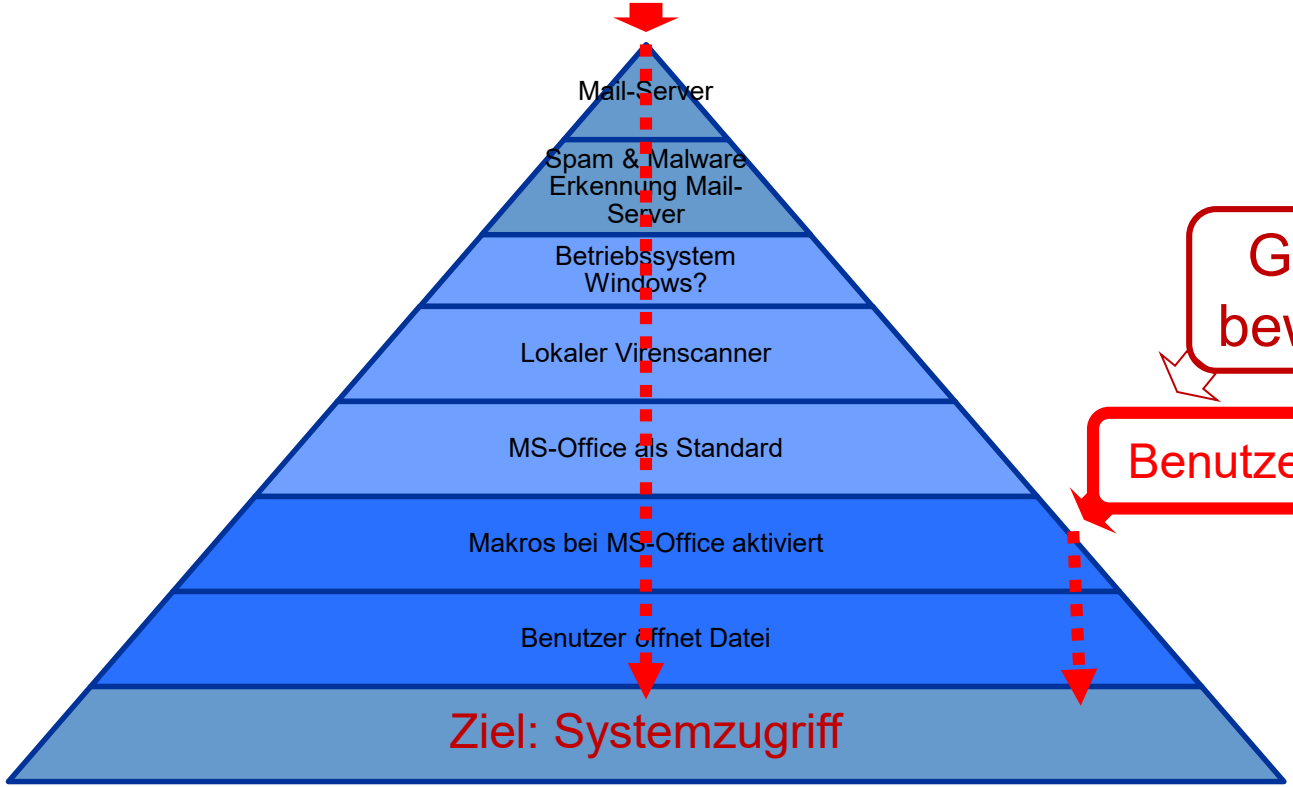
Please find the pictures attached.

Please also find a picture containing my **account details**.

Seen, thanks. I will get back to you soon.

END OF STORY

Gegenmaßnahmen auf diversen Ebenen:



Aktuelles 2020/21

- Weitere Professionalisierung
  - Befreiung von Trojanern und Absicherung gegen zukünftige Angriffe als „Dienstleistung“ (zusätzlich zur Entschlüsselung)
  - „Callcenter“ für Support während der Abwicklung
  - Ausnahme von öffentlicher Infrastruktur (Medizinische Versorgung, Universitäten)

Aktuelles 2020/21 – Gefahren durch Covid-19

- Änderung der IT-Nutzung:
  - Deutlicher Anstieg der Remote-Nutzung
    - Größeres Angriffspotential durch
      - Ermöglichung weltweiter Zugriffe
      - Benutzung privater (und damit unkontrollierbarer) Endgeräte
      - „Offline-Nutzung“ schützenswerter Daten auf ungesicherten Geräten
  - „Neue“ Kommunikationswege (Video-Konferenzen, etc.)
    - Cloud-Basierte Lösungen: Skalierbarkeit contra Datenschutz
    - Sicherheitsprobleme bei eingesetzten Produkten

Was wäre wenn…

- … während des Corona-Online-Semesters einem massiven Trojaner-Befall ausgesetzt wäre?

RRZE-Veranstaltungskalender und Mailinglisten

- Anleitung Kalender abonnieren oder bookmarken
  - www.rrze.fau.de/veranstaltungen/veranstaltungskalender/

- Mailingliste abonnieren
  - Wöchentliche Terminhinweise werden zusätzlich an die Mailingliste RRZE-Aktuelles gesendet.
  - Auch diese Liste kann man abonnieren: https://lists.fau.de/mailman/listinfo/rrze-aktuelles