Datenschutzschulung für Mitarbeiter:innen

Datenschutz

Webex, März 2023, Montanuniversität Leoben

UNTERNEHMENSGRUPPE

Vorstellung

Mag. iur. Martina Wenghofer MA

Datenschutzjuristin

bei x-tention Informationstechnologie GmbH

Ausbildung

Studium der Rechtswissenschaften

Studium IT-Recht und Management

Zertifizierungen

Datenschutzbeauftragter (WIFI - Wirtschaftsförderungsinstitut)

xtention
IT with care.

Agenda

01 Datenschutz – Kurze Einführung

02 DSGVO - Betroffenenrechte

03 DSGVO - Datenschutzvorfälle

04 Social Engineering

05 Sicherheit von E-Mails

06 Hackerangriffe

07 Lessons Learned

01

Datenschutz

Kurze Einführung

Datenschutz

Was ist Datenschutz?

- Schutz der Privatsphäre
- Freiheit der Menschen, ihre Daten selbst zu bestimmen (informationelle Selbstbestimmung)

Warum brauchen wir Datenschutz?

Ich hab doch nichts zu verbergen!?

- Privatsphäre
- Ob man etwas zu verbergen hat, liegt im Auge des Betrachters
- Private Daten haben einen Wert
- Datensparsamkeit (Data Minimization) ist Risikominimierung
- Gelegenheit macht Datendiebe
- Was heute harmlos ist, ist es morgen vielleicht nicht mehr

Wie viel verdienen Sie?

Darf ich Ihr E-Mail-Passwort haben?

Wozu sollen Sie Ihre Haustüre absperren?

Was haben Sie diese Woche eingekauft?

Wenn Sie jemanden 24h beobachten würde, würden Sie etwas an Ihrem verhalten ändern?

DSGVO

Welche Arten von Daten schützt die DSGVO?

- Personenbezogene Daten
- Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen

Name

IP-Address

Telefonnummer

Geburtsdatum

E-Mail-Addresse

Nummernschild

Krankenstand

Gesundheitsdaten

Haut-,Haar-, Augenfarbe

Urlaubsplanung

Job

Familienstand

Addresse

Einkommen

Kleidergröße

Vermögenssituation

Ausbildung

Solzialversicherungsnummer

Steurnummer

Religionsbekenntnis

Bankverbindung

DSGVO

Welche Arten von Daten schützt die DSGVO?

- Besondere Kategorien von Daten
  - Rasse oder ethnische Herkunft
  - Politische Meinungen
  - Religiöser oder philosophischer Glaube
  - Gewerkschaftsmitgliedschaft
  - Genetische Daten
  - Biometrische Daten
  - Sexuelle Orientierung
  - Gesundheitsdaten

Die Verarbeitung dieser Art von Daten ist nur unter bestimmten Umständen erlaubt und muss mit besonderer Sorgfalt behandelt werden.

DSGVO

Welche Arten von Daten schützt die DSGVO?

- Pseudonymisierung
  - Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne die Verwendung zusätzlicher Informationen nicht mehr einer bestimmten betroffenen Person zugeordnet werden können
  - zusätzliche Informationen müssen gesondert aufbewahrt werden und unterliegen technischen und organisatorischen Maßnahmen, um sicherzustellen, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugeordnet werden
- Anonymisierung
  - Verarbeitung der Entfernung aller persönlichen Identifikatoren, die zu einer Person führen könnten

Pseudonyme Daten sind ebenfalls personenbezogene Daten und fallen in den Anwendungsbereich der DSGVO!

DSGVO

Rollen/Beteiligte

- Betroffener
  - natürliche oder natürliche Person, die Gegenstand personenbezogener Daten ist
- Verantwortlicher
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; Sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten bestimmt, so können der Verantwortliche oder die spezifischen Kriterien für seine Benennung im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehen werden
- Auftragsverarbeiter
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des für die Verarbeitung Verantwortlichen verarbeitet

DSGVO

Rollen/Beteiligte

- Empfänger
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, gegenüber der die personenbezogenen Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen einer bestimmten Untersuchung im Einklang mit dem Unionsrecht oder dem Recht der Mitgliedstaaten personenbezogene Daten erhalten können, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch diese Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften entsprechend den Zwecken der Verarbeitung
- Dritter
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten

02

DSGVO

Betroffenenrechte

DSGVO

Betroffenenrechte

Recht auf Auskunft (Art. 15)

- Der Betroffene kann Auskunft über die personenbezogenen Daten verlangen, die über ihn verarbeitet werden.

Recht auf Berichtigung (Art. 16)

- Falls Informationen fehlerhaft sind, kann der Betroffene die Richtigstellung verlangen.

Recht auf Löschung (Art. 17)

- Der Betroffene kann verlangen, dass Daten, die ihn betreffen, unverzüglich gelöscht werden.
- Dies gilt nur, wenn dem keine gesetzlichen Verpflichtungen entgegenstehen wie z.B. die gesetzliche Aufbewahrungspflicht von Vertragsdaten von 7 Jahren oder von Gesundheitsdaten von 30 Jahren.

DSGVO

Betroffenenrechte

Recht auf Einschränkung der Verarbeitung (Art. 18)

- Die betroffene Person hat das Recht unter bestimmten Umständen die Einschränkung der Verarbeitung ihrer personenbezogenen Daten zu verlangen.

Recht auf Datenübertragbarkeit (Art. 20)

- Der Betroffene hat das Recht, seine personenbezogenen Daten in einer strukturierten, gängigen und maschinenlesbaren Form zu erhalten oder diese an einen anderen Verantwortlichen übermitteln zu lassen.

Recht auf Widerspruch (Art. 21)

- Die betroffene Person hat das Recht, unter bestimmten Umständen gegen die Verarbeitung sie betreffender personenbezogener Daten Widerspruch einzulegen.

DSGVO

Behandlung von Betroffenenrechten

Wo können Anträge auf Betroffenenrechte gestellt werden?

- Bei jedem/jeder Mitarbeiter:in der Montanuniversität Leoben

Wieviel Zeit bleibt zur Bearbeitung eines Betroffenenantrags?

- Ab Einlangen des Betroffenenantrags 4 Wochen
- Eine Verlängerung der Frist kann nur in begründeten Fällen erfolgen

Was müssen Sie tun, wenn ein Antrag bei Ihnen gestellt wird?

- Den Eingang des Antrags umgehend unter dsb@unileoben.ac.at melden!
- Danach wird das weitere Vorgehen mit Ihnen, der Datenschutzkoordination und der Datenschutzbeauftragten abgestimmt.

03

DSGVO

Datenschutzvorfälle

DSGVO

Datenschutzverletzung = Datenschutzvorfall

Definition

- Datenschutzverletzung: Verletzung des Schutzes personenbezogener Daten.
- Identifizierte Datenschutzvorfälle sind unverzüglich weiterzuleiten!
- Meldung innerhalb von 72 Stunden an die Datenschutzbehörde, wenn ein Risiko für betroffene Person besteht.

Beispiele für Datenschutzverletzungen

- Unerwünschte Veröffentlichung von personenbezogenen Daten im Internet
- Versehentliches Versenden von personenbezogenen Daten an falsche Empfänger
- Verlust oder Diebstahl von Datenträgern
- Weitergabe personenbezogener Daten an unbefugte Dritte

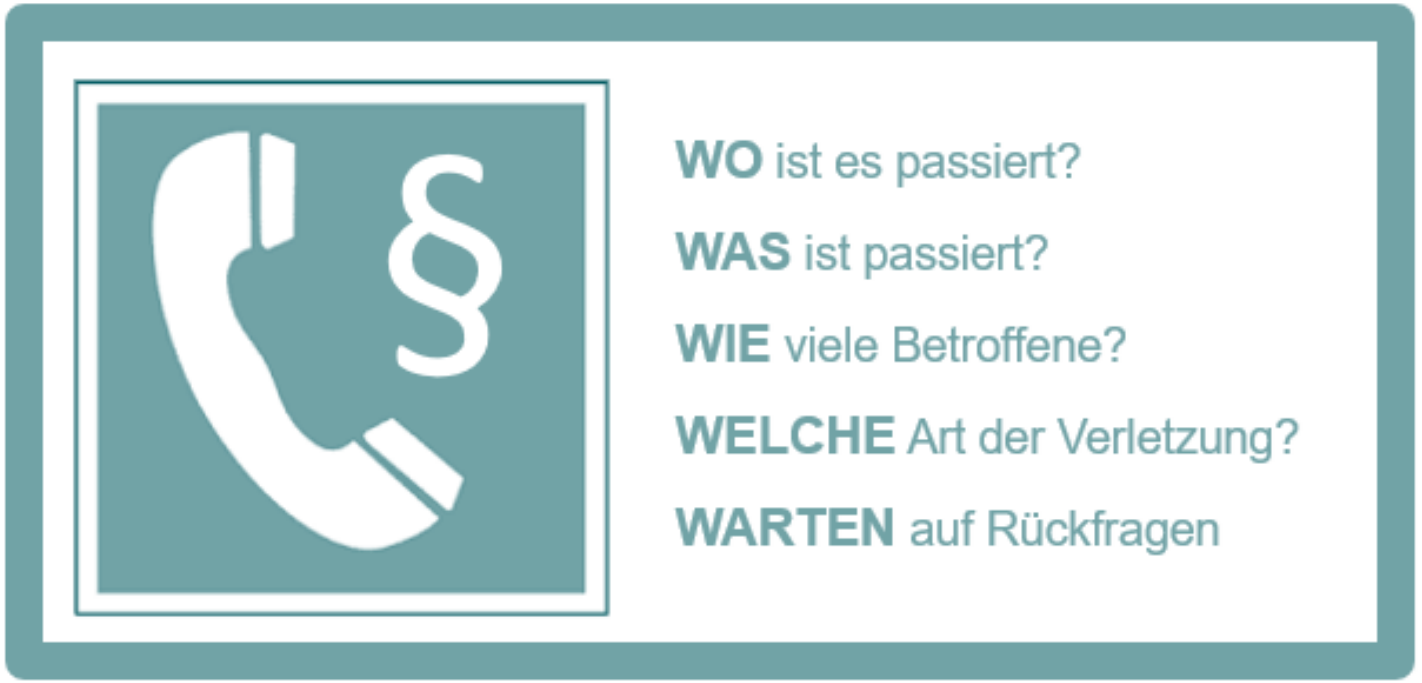
DSGVO

Datenschutzvorfälle – Nützliche Links

- https://haveibeenpwned.com/ - waren meine Daten Teil eines Data Breaches
- https://www.watchlist-internet.at/ - Auflistung der Jüngsten Fishing Attacken

Datenschutzvorfälle

Welche Informationen sind zu melden?



DSGVO

Ansprechpartner bei Datenschutzangelegenheiten

Datenschutz-Koordinator

- Interne Ansprechperson für Datenschutz
- Anlaufstelle für Betroffenenrechte und Datenpannen
- Regelmäßige Aktualisierung und Verbesserung des Datenschutz-Managementsystems

Dr. Klaus Sapetschnig

+43 3842/402-7002

dsb@unileoben.ac.at

Datenschutzbeauftragter

- Unterrichtet und berät zum Thema Datenschutz
- Überwachung der Einhaltung Datenschutzvorschriften
- Schulung der an Verarbeitungsvorgängen beteiligten Mitarbeiter
- Zentrale Anlaufstelle für die Datenschutzbehörde

Fa. x-tention Informationstrechnologie GmbH

Service.Datenschutz@x-tention.at

04

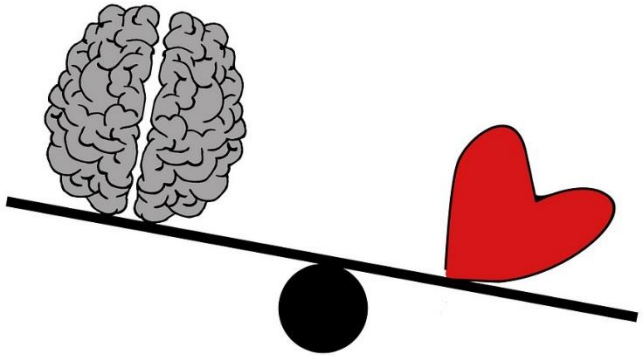
Social Engineering

Mitarbeiter als Angriffsziel

Was ist Social Engineering?

Ausnutzen **menschlicher Eigenschaften**, um an Informationen zu kommen

Hilfsbereitschaft
Kundenfreundlichkeit
Dankbarkeit
Gutgläubigkeit
Respekt vor Autoritäten
Konfliktvermeidung
Wunsch, guter Teamplayer zu sein



Effiziente Methode zur Informationsbeschaffung meist ohne Einsatz technischer Hilfsmittel

Häufig die einfachste Form des Angriffs

Psychologie steht im Vordergrund

Meist zur Vorbereitung für einen Hackerangriff

Beispiele aus der Praxis

Anruf vom „Administrator“ (z.B. Microsoft-Mitarbeiter)

Verlangt Informationen über bestimmte Systeme

… oder Auskunft über Passwort

Gefundener USB-Stick am Parkplatz

Wird bewusst ausgelegt

Infiziert mit Schadsoftware

Aufhalten bzw. Aufsperren von zutrittsgesicherten Türen (z.B. Lieferant, Techniker)

Hilfsbereitschaft

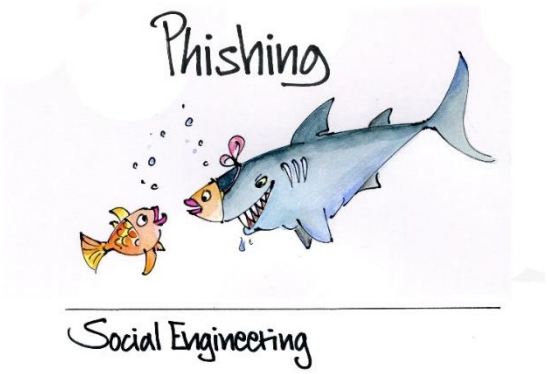
Leerstehende Büros mit offenen Türen

Gespräch im Freundeskreis (Wirtshaus etc.)

Weitererzählen von Infos über Patienten, neue Technologien usw.

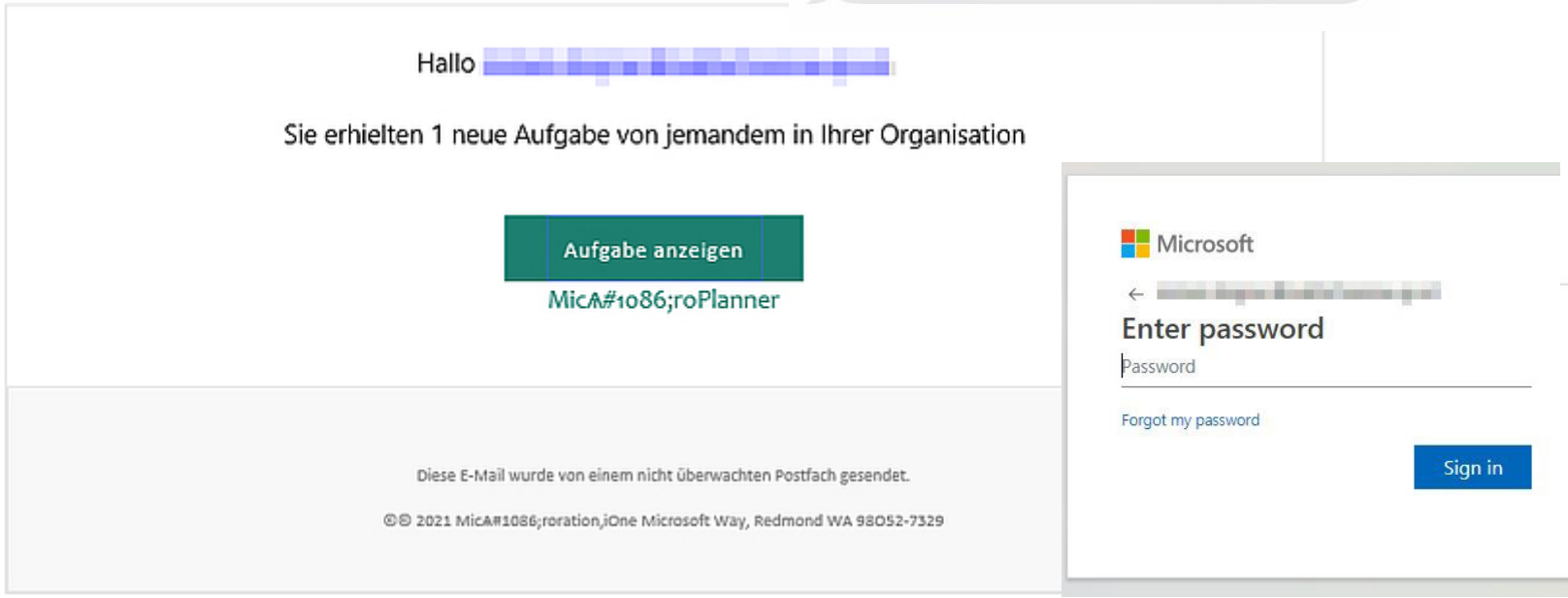
CEO Fraud

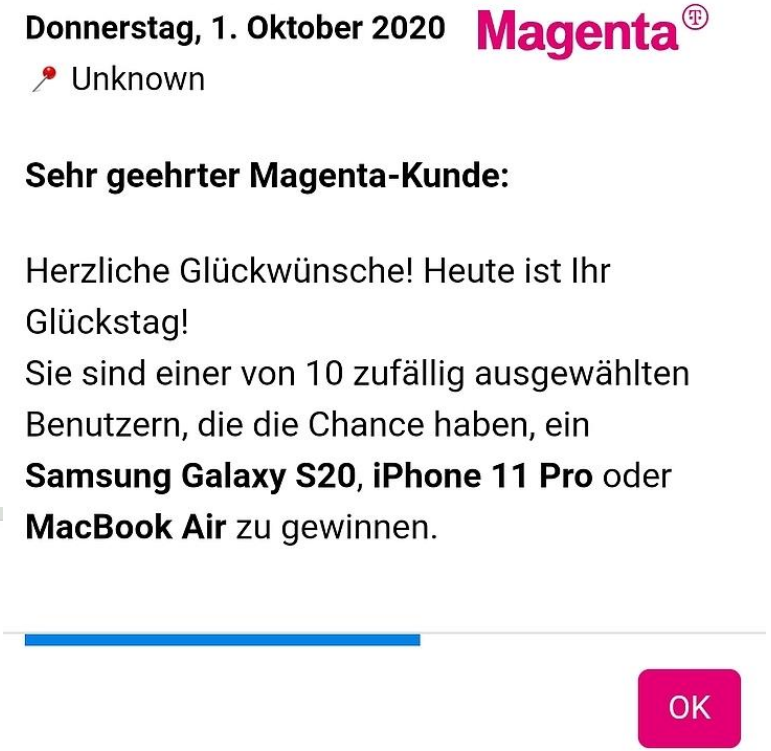
E-Mail vom „Chef“ zum Überweisen von hohen Geldbeträgen



Quelle: https://www.presseportal.de/pm/58214/2885887

Beispiele aus der Praxis





Schutz vor Social Engineering

Hausverstand nutzen!

Würde mein Chef am Telefon wirklich verlangen, dass ich ihm mein Passwort weitergebe?

Warum ruft mich jemand an, der von mir wissen möchte, welche Schlüssel / Zutrittskarten / Betriebssysteme / Programme wir verwenden?

Seien Sie skeptisch gegenüber Fragen Unbekannter!

Rückruf verlangen!

Rufen Sie den Anrufer auf die im System hinterlegte bzw. die Ihnen bekannte Nummer zurück

Passwörter niemals weitergeben!

z.B. PINs, TANs, Passwörter

Sprechen Sie unbekannte Personen in sensiblen Bereichen an!

05

Sicherheit von E-Mails

Wie erkenne ich Spam- und Phishing-Mails?

Was ist Phishing?

Ein Angreifer versucht, über …

gefälschte Webseiten,

gefälschte E-Mails oder

gefälschte Nachrichten

… an persönliche Daten zu gelangen (Identitätsdiebstahl)

Mögliche Folgen

Kontoplünderung

Datenverschlüsselung

Datenzerstörung

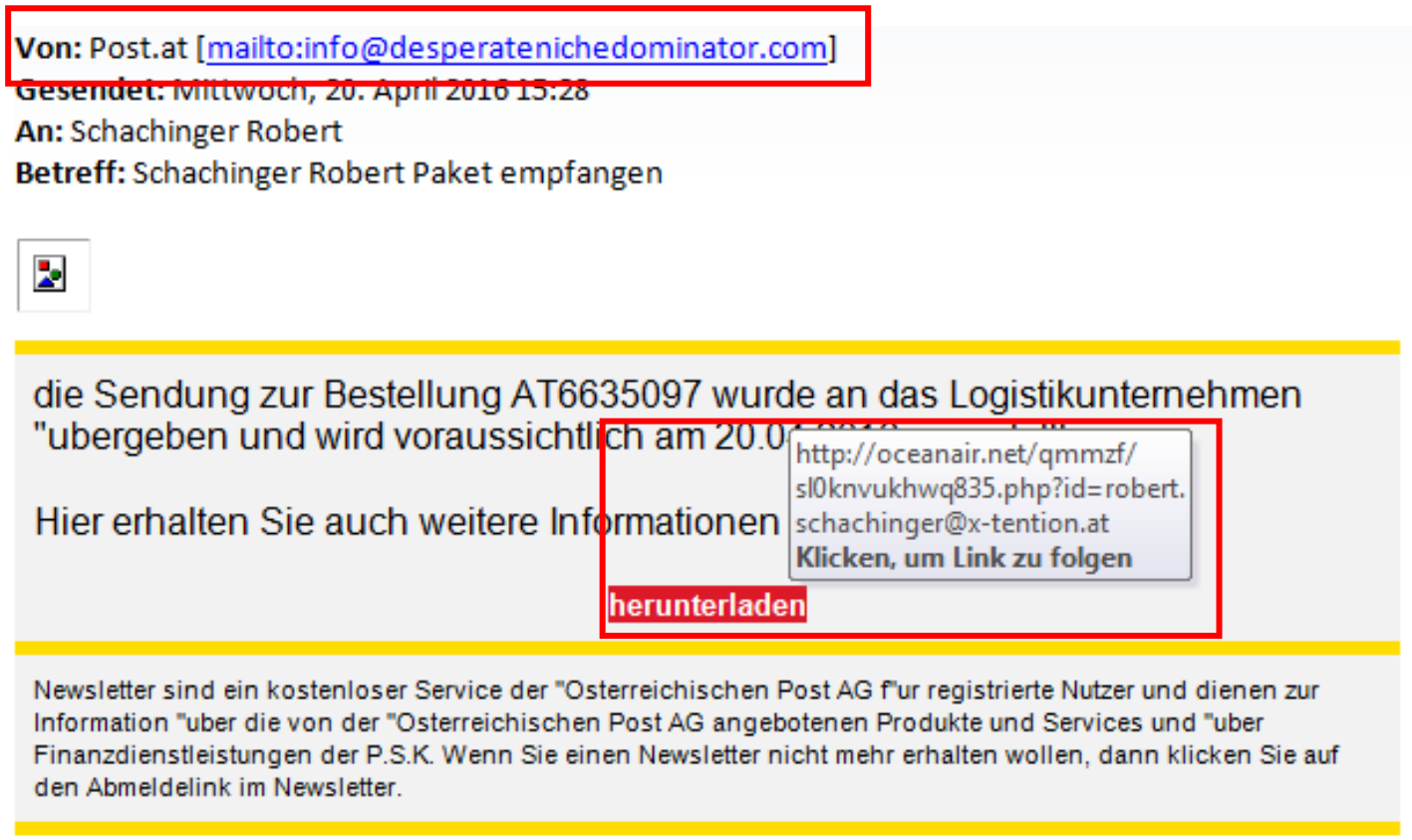
Erpressung

usw.

Bildquelle: pixabay.com

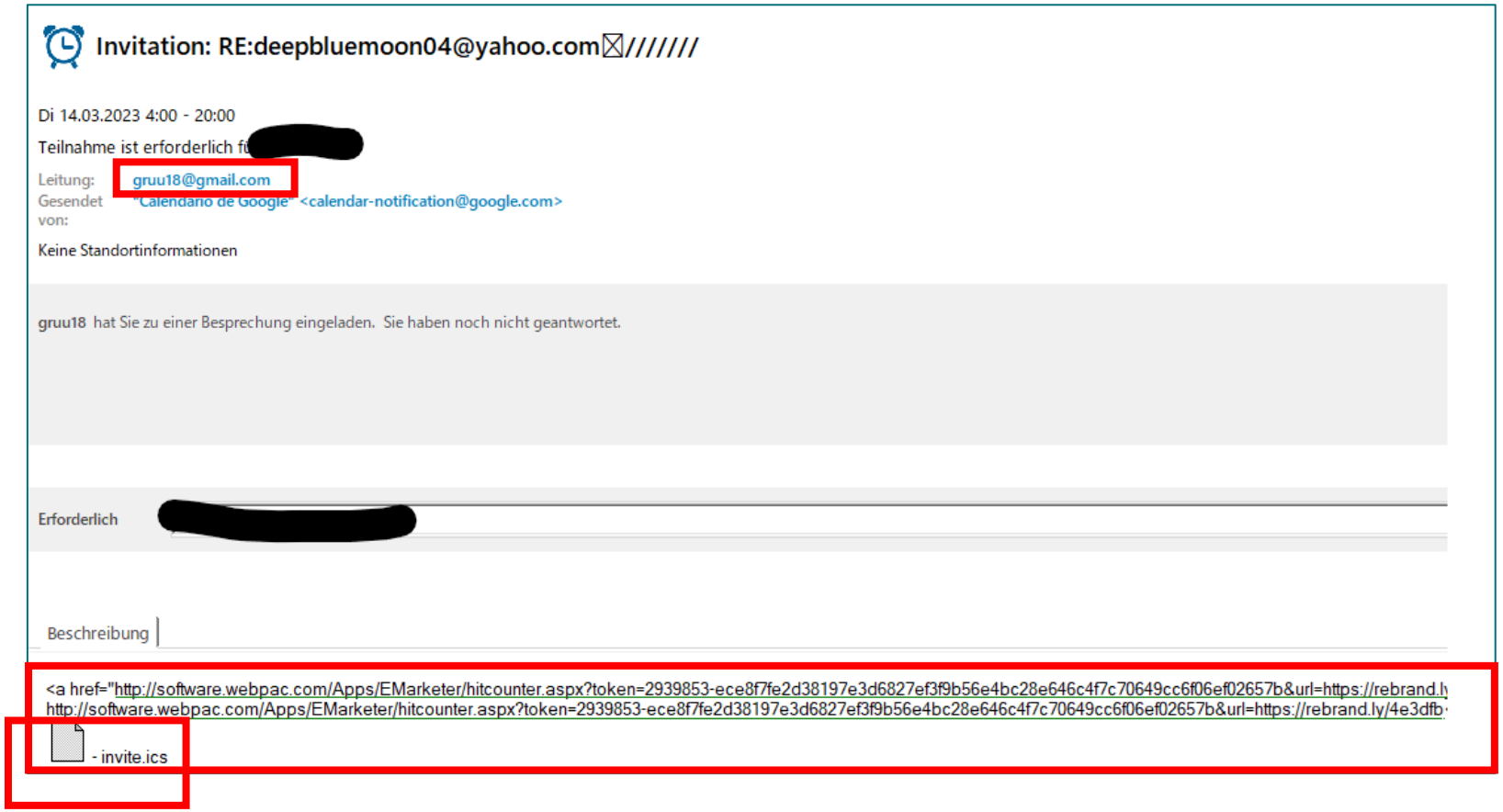
Wie kann ich mich schützen?

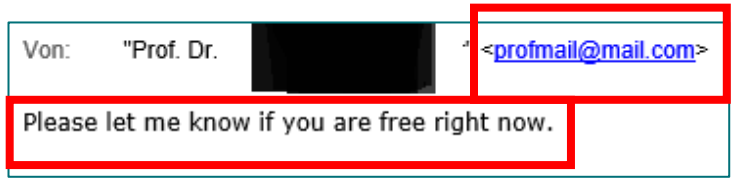
- E-Mails aufmerksam lesen (Rechtschreib- und Tippfehler)
- Kritisch hinterfragen, warum Sie bestimmte Mails bekommen
- Werden sensible Informationen abgefragt (z.B. PIN, Kontonummer)
- Absender-Adresse der E-Mail prüfen
- ACHTUNG: Angezeigter Namen ≠ Tatsächlicher Absender
- Link-Adresse im Mail kontrollieren
- ACHTUNG: Nur mit der Maus über den Link fahren, NICHT anklicken!
- Unbekannte Anhänge NICHT öffnen (z.B. Rechnungen)
- Siehe auch: www.watchlist-internet.at



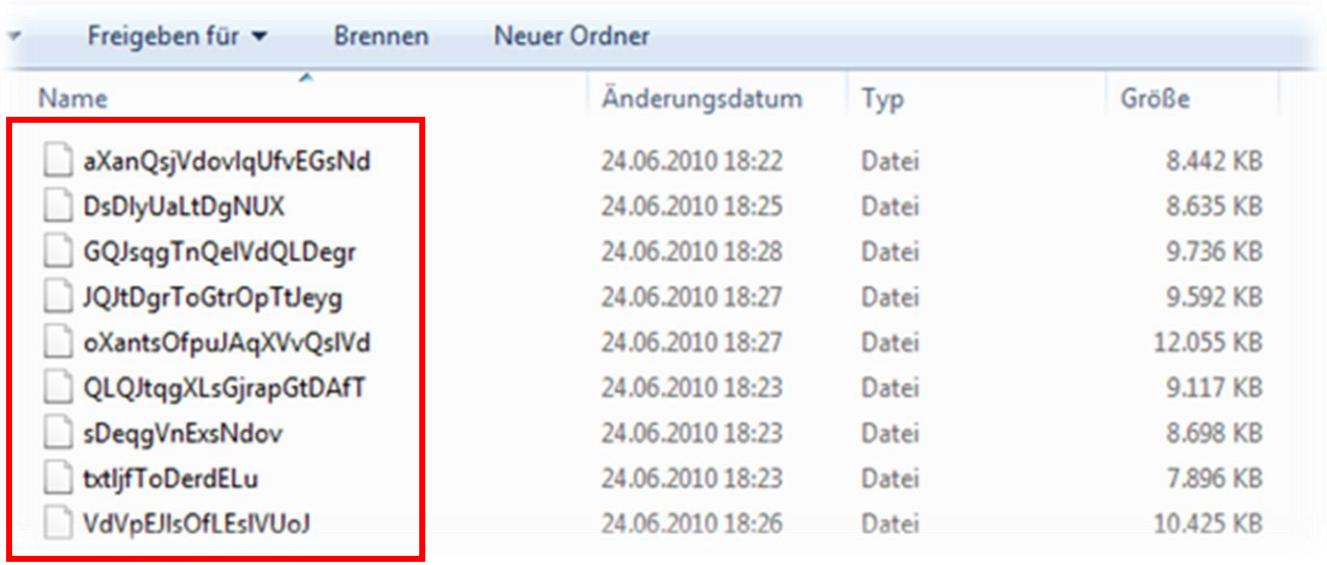
Beispiele an der MUL

Phishingmails





Und wenn‘s doch passiert?



Vertrauensperson aus der IT und aus dem Datenschutz umgehend informieren!

06

Hackerangriffe

Kurze Einführung und aktuelle Beispiele

Einführung

Definitionen

Was ist Hacking?

- Aktivitäten, bei denen versucht wird, digitale Geräte wie Rechner, Smartphones, Tablets oder ganze Netzwerke zu kompromittieren.

Was sind Gründe für Hackergangriffe?

- Finanzielle Motive (Bereicherung)
- Image innerhalb der Hackerszene
- Wirtschaftliche Motive (Betriebsspionage)
- Politische Motive

Welche Arten von Hackern gibt es?

- White-Hat-Hacker: „gute Hacker“, deren Ziel es ist, Sicherheitssystemen zu verbessern
- Black-Hat-Hacker: „böse Hacker“, die durch kriminelle Aktivitäten Schaden erzeugen möchten
- Grey-Hat-Hacker: „ein bisschen was von beiden Hacker“, die in Systeme eindringen ohne kriminellen Schaden zu erzeugen und dem Betroffenen die Schwachstellen aufzeigen und gegen Geld beseitigen

Aktuelle Hackerangriffe gegen Hochschulen

Hackerangriff Med-Uni: Polizei ermittelt

Hacker haben die IT-Infrastruktur der Medizinischen Universität Innsbruck angegriffen und teilweise lahmgelegt. Interne und externe Spezialisten würden derzeit intensiv an der Schadensbehebung arbeiten. Daneben ermittelt auch die Polizei.

Versuchter Hackerangriff auf Uni Innsbruck

Unbekannte Täter haben am Wochenende versucht, in die IT-Infrastruktur der Landesuniversität einzudringen. Ein größerer Schaden dürfte nach derzeitigem Stand nicht entstanden sein, hieß es von der Universität. Der Cyberangriff sei rasch bemerkt worden.

Cyber-Angriff: IT der TU Freiberg weitreichend lahmgelegt

Ein Cyber-Angriff auf die IT der TU Freiberg in Sachsen führt zu weitreichenden Einschränkungen. Zum Wochenende hat die Uni die Internetverbindungen gekappt.

Uni Salzburg: Hackerangriff legt E-Mail-Server lahm

Jetzt hat es auch die Uni Salzburg erwischt: In der Nacht von Sonntag auf Montag haben Hacker die Email-Accounts attackiert. Rund 3.000 Email-Adressen wurden deshalb offline gestellt. Experten sind seither damit beschäftigt, den Umfang des Schadens zu erheben.

Hackerangriff auf Uni Graz: Experten am Zug

Nach dem Hackerangriff auf das IT-Netzwerk der Universität Graz am Freitag arbeiten die IT-Expertinnen und Experten auf Hochtouren, um das Ausmaß des Cyberangriffs zu erheben. Man rechne Ende der Woche mit Ergebnissen. Die Datenschutzbehörde wurde informiert.

Cyberangriff: TU Berlin rechnet mit monatelangen IT-Einschränkungen

Es wird noch einige Zeit dauern, bis die zentralen IT-Systeme der TU Berlin nach der Ransomware-Attacke wieder laufen. Auch das SAP-Kernsystem ist betroffen.

Warum Angriffe auf Bildungseinrichtungen?

Was macht Hochschulen als Ziel so attraktiv?

- Hochschulen sammeln und sichern eine große Menge personenbezogener Daten von Studierenden, Mitarbeiter:innen, Forschungsstudienteilnehmer:innen uvm..
- Hochschulen speichern und verwalten wertvolles geistiges Eigentum – Forschungsdaten und – ergebnisse.
- Der Umstieg bzw. Aufschwung der Digitalisierung von Hochschulen in der Pandemie erfolgte sehr schnell. Risiken in Punkto Cybersicherheit werden dadurch erst nach und nach bekannt und müssen budgetär berücksichtigt werden.
- Angriffe auf Bildungseinrichtungen sollen oft auch destabilisierende Wirkung für die Gesellschaft haben.

Welche Angriffsmethoden kommen zum Einsatz?

Wie wird angegriffen?

- Fishing-Angriffe (um Benutzernamen und Passwörter abzugreifen)
- Spam (Störung von E-Mail-Servern; Kompromittierung von MUL-E-Mailadressen)
- Malware-Angriffe (Software, die unerwünschte oder sogar schädliche Funktionen ausführt
  - Ransomware (verschlüsselt Daten auf Systemen – meist mit Erpressung verbunden)
- Denial-of-Service-Attacken (Systemüberlastung durch absichtliche Überflutung eines Netzwerks mit gefälschtem Datenverkehr)

07

Lessons Learned

Lessons Learned

Was gibt's zu merken?

1. Datenschutz ist wichtig!
2. Anträge auf Betroffenenrechte melden!
3. Datenschutzvorfälle melden!
4. Bei verdächitgen E-Mails nie auf Links klicken oder Anhänge öffnen!
5. Cyberattacken sind schon mit geringem Aufwand möglich (Social Engeneering, Fishing-E-Mails).
6. Hochschulen werden für Angriffe immer attraktiver.
7. Nützliche Links:
   - https://haveibeenpwned.com/
   - https://www.watchlist-internet.at/
8. Für Datenschutzfragen wenden Sie sich bitte an dsb@unileoben.ac.at .

Zeit für Fragen ☺

Vielen Dank

x-tention Informationstechnologie GmbH
Römerstraße 80a, 4600 Wels, Austria
Service.Datenschutz@x-tention.com

IT with care.