

Datenschutzschulung für Mitarbeiter:innen

Datenschutz

Webex, September 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)



x-tention
IT with care.

Agenda

01

Datenschutz – Kurze Einführung

02

DSGVO - Betroffenenrechte

03

DSGVO - Datenschutzvorfälle

04

Social Engineering – aktuelle Beispiele

05

Watchlist Internet – 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)

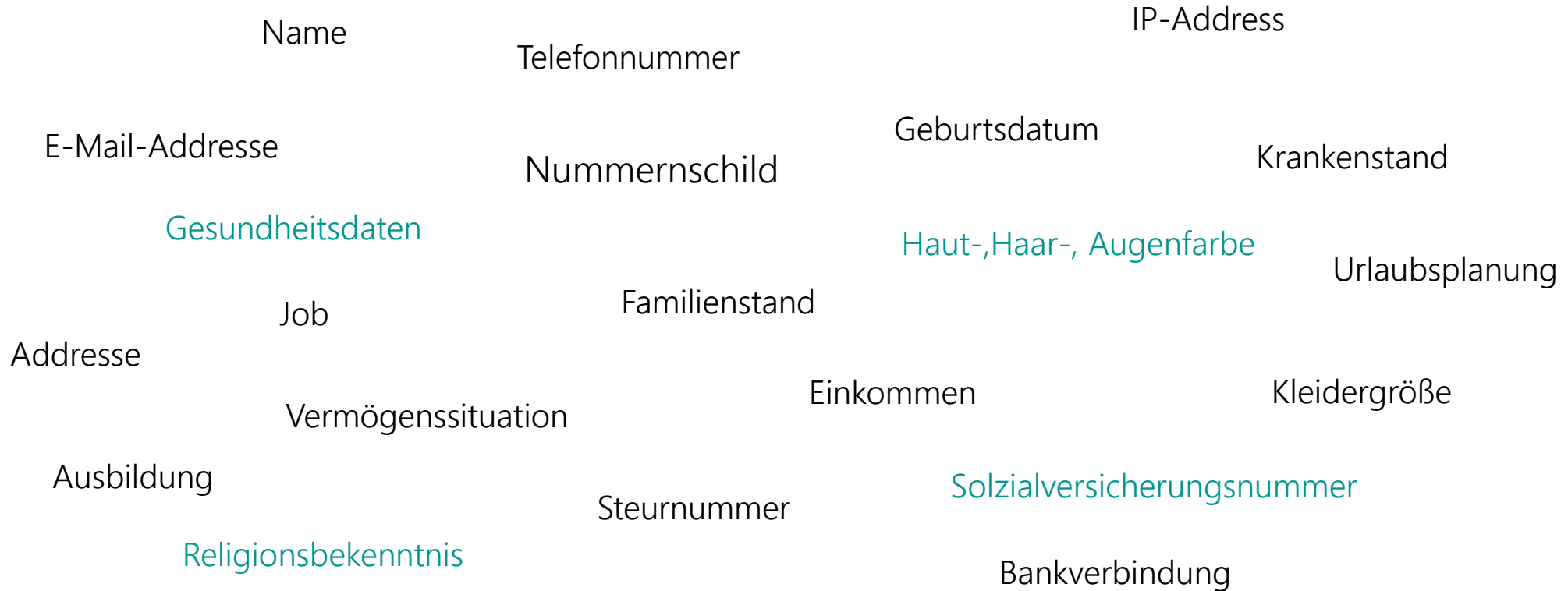


DSGVO

Welche Arten von Daten schützt die DSGVO?



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



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 Attacks

Datenschutzvorfälle

Welche Informationen sind zu melden?



WO ist es passiert?

WAS ist passiert?

WIE viele Betroffene?

WELCHE Art der Verletzung?

WARTEN auf Rückfragen

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 Informationstechnologie GmbH



Service.Datenschutz@x-tention.at



04

Social Engineering

Aktuelle Beispiele

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



© Social Engineering - snapSEC - IT-Sicherheit und Datenschutz

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

Aktuelle Beispiele

Internetbetrug: Pensionist verliert 14.500 Euro

Ein 69-jähriger Vorarlberger ist Opfer von Internetbetrügern geworden. Er klickte im Internet auf eine Werbeanzeige mit dem Titel „Reich werden mit 250 Euro“. Reich wurde er nicht – im Gegenteil. Der Pensionist wurde um 14.500 Euro erleichtert.

Betrug über Verkaufsplattform

Zwei Frauen sind über Verkaufsplattformen im Internet betrogen worden. Der Schaden beträgt in beiden Fällen mehrere tausend Euro. Beide Frauen wollten Kleidungsstücke verkaufen und wurden dabei betrogen.

21-Jährige Opfer von Internetbetrug

Eine junge Frau in Kramsach ist Opfer eines Internetbetruges geworden. Sie erhielt eine angebliche SMS ihrer Bank und folgte einem Link im Internet. Die Frau wurde um einen vierstelligen Eurobetrag gebracht. Das Bundeskriminalamt warnt vor einer Betrugswelle.

Kapellen im Visier von Betrügern

Derzeit wird in Österreich betrügerisch versucht, bei Blasmusikkapellen an Geld zu gelangen. Konkret wurde das unter anderem bei der Stadtkapelle Gmunden versucht. Die Täter geben sich in einer gefälschten E-Mail als Geschäftsführer von Firmen aus und verschicken Rechnungen.

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

Watchlist Inernet

Sicherheit von E-Mails, Messenger-Nachrichten

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 \neq 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

Von: Post.at [<mailto:info@desperatenichedominator.com>]

Gesendet: Mittwoch, 20. April 2016 15:28

An: Schachinger Robert

Betreff: Schachinger Robert Paket empfangen



die Sendung zur Bestellung AT6635097 wurde an das Logistikunternehmen "übergeben und wird voraussichtlich am 20.07.2016 an Sie

Hier erhalten Sie auch weitere Informationen


<http://oceanair.net/qmmzf/sl0knvukhwq835.php?id=robert.schachinger@x-tention.at>
Klicken, um Link zu folgen

herunterladen

Newsletter sind ein kostenloser Service der "Österreichischen Post AG" für registrierte Nutzer und dienen zur Information über die von der "Österreichischen Post AG" angebotenen Produkte und Services und über Finanzdienstleistungen der P.S.K. Wenn Sie einen Newsletter nicht mehr erhalten wollen, dann klicken Sie auf den Abmeldelink im Newsletter.

Beispiele an der MUL

Phishingmails

 Invitation: RE:deepbluemoon04@yahoo.com ☒////////

Di 14.03.2023 4:00 - 20:00

Teilnahme ist erforderlich für [REDACTED]

Leitung: gruu18@gmail.com

Gesendet: "Calendar de Google" <calendar-notification@google.com>

von:


Keine Standortinformationen

gruu18 hat Sie zu einer Besprechung eingeladen. Sie haben noch nicht geantwortet.

Erforderlich [REDACTED]

Beschreibung |

<http://software.webpac.com/Apps/EMarketer/hitcounter.aspx?token=2939853-ece8f7fe2d38197e3d6827ef3f9b56e4bc28e646c4f7c70649cc6f06ef02657b&url=https://rebrand.ly/4e3dfb>

 - invite.ics

Von: "Prof. Dr. [REDACTED]" <profmail@mail.com>

Please let me know if you are free right now.

Beispiele an der MUL

Phishingmails

Von "██████████" <██████████@unileoben.ac██████████.com>
An ██████████@unileoben.ac.at
Bitte Antwort an "██████████" <██████████@ceo-gmbh.me>

Hallo ██████████

Haben wir ein Tageslimit für internationale Expresszahlungen? Können wir heute 46 tausend zahlen?

LG
██████████

Von: "Montanuniversität Leoben" <██████████@students.zcu.cz>
Datum: 11.11.2022 10:22
Betreff: [EXT] Fehlgeschlagene Nachrichten (3)

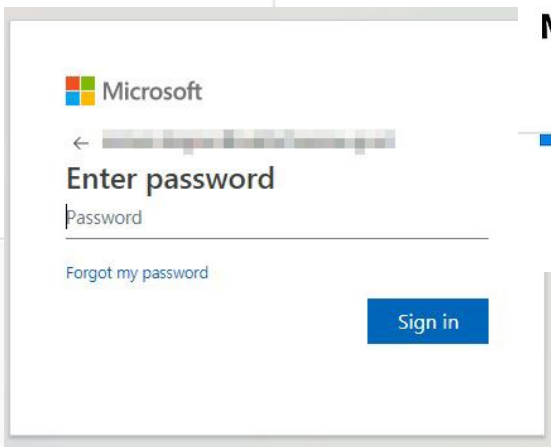
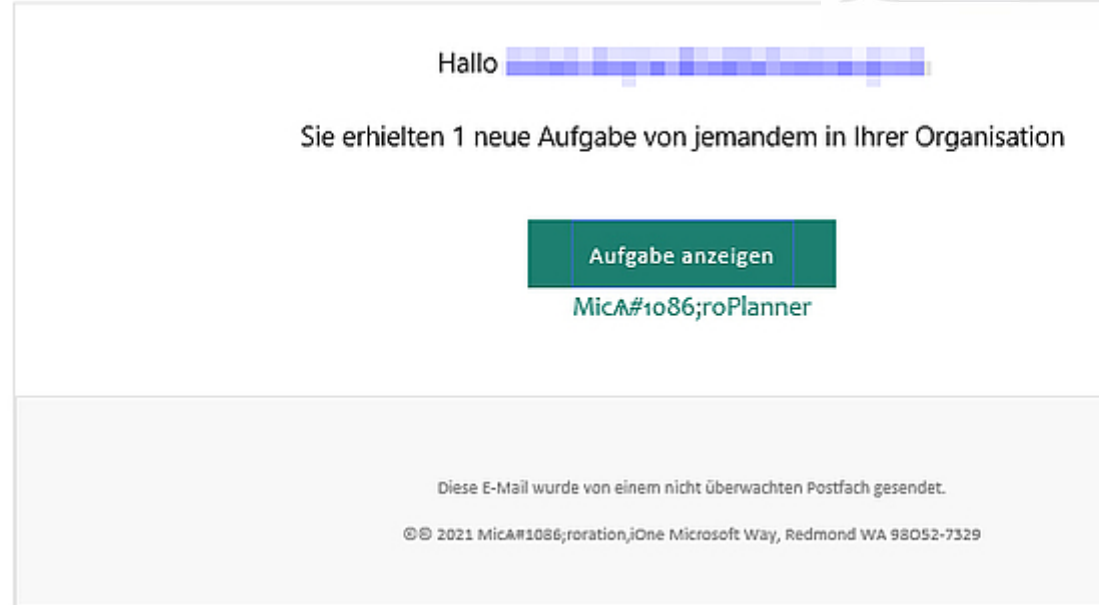
ATTN: ██████████@unileoben.ac.at
Um 10:10 wurden 3 neue E-Mails an den Absender zurückgeschickt.

Klicken Sie unten, um eine Vorschau der fehlgeschlagenen Nachrichten anzuzeigen.

[Fehlgeschlagene Nachrichten abrufen](#)

© 2022 Montanuniversität Leoben.

Beispiele aus der Praxis



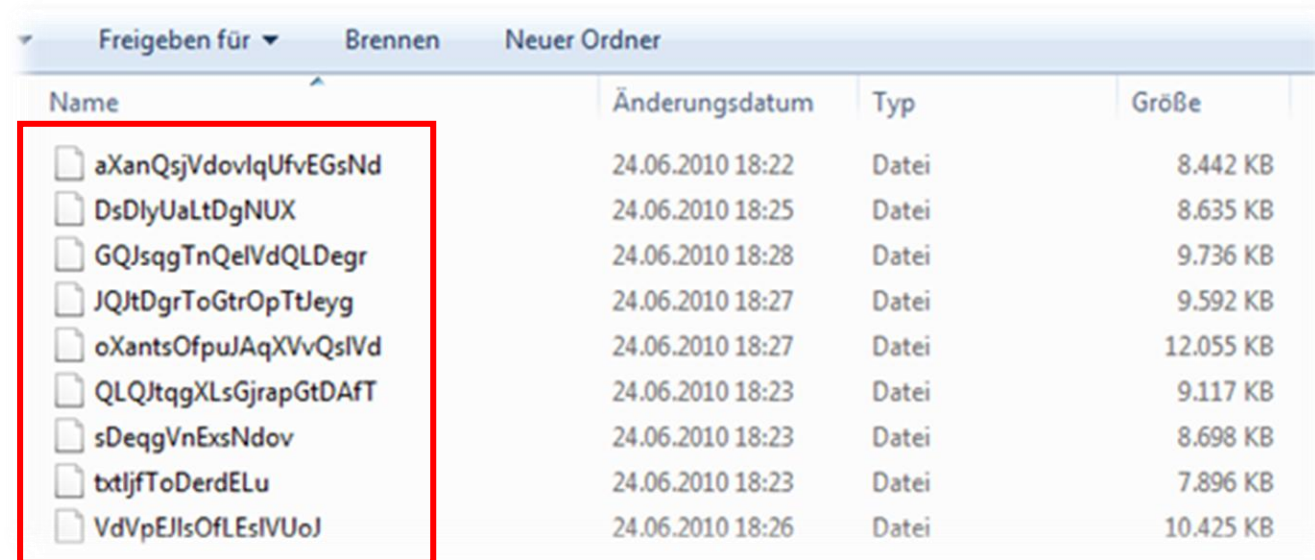
Donnerstag, 1. Oktober 2020 **Magenta**[®]
📍 Unknown

Sehr geehrter Magenta-Kunde:

Herzliche Glückwünsche! Heute ist Ihr Glückstag!
Sie sind einer von 10 zufällig ausgewählten Benutzern, die die Chance haben, ein **Samsung Galaxy S20, iPhone 11 Pro** oder **MacBook Air** zu gewinnen.



Und wenn's doch passiert?



Name	Änderungsdatum	Typ	Größe
aXanQsjVdovlqUfvEGsNd	24.06.2010 18:22	Datei	8.442 KB
DsDlyUaLtDgNUX	24.06.2010 18:25	Datei	8.635 KB
GQJsqgTnQelVdQLDegr	24.06.2010 18:28	Datei	9.736 KB
JQJtDgrToGtrOpTtJeyg	24.06.2010 18:27	Datei	9.592 KB
oXantsOfpuJAqXVvQsIVd	24.06.2010 18:27	Datei	12.055 KB
QLQJtqgXLsGjrapGtDAfT	24.06.2010 18:23	Datei	9.117 KB
sDeqqVnExsNdov	24.06.2010 18:23	Datei	8.698 KB
txtljfToDerdELu	24.06.2010 18:23	Datei	7.896 KB
VdVpEJIsOfLEsIVUoJ	24.06.2010 18:26	Datei	10.425 KB



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 verdächtigten E-Mails nie auf Links klicken oder Anhänge öffnen!
5. Cyberattacken sind schon mit geringem Aufwand möglich (Social Engineering, Fishing-E-Mails).
6. Hochschulen werden für Angriffe immer attraktiver.
7. Nützliche Links:
 - <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

xtention
IT with care.