MEDIZINISCHE UNIVERSITÄT
INNSBRUCK

Handout zum Kompaktworkshop Informationssicherheit

Mag. Christoph Riesenfelder, CISM, CPP, CISSP, SSCP, ISMS LA, CRISC

http://www.riesenfelder.com

Version 0.6

Inhaltsverzeichnis

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Das Symbol rechts auf jeder Seite bedeutet:

Zurück zum Inhaltsverzeichnis

Kapitelende – zurück zum Inhaltsverzeichnis

Wichtige Begriffe in dieser Unterlage

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- **Datenschutz**: Stellt sicher, dass die Verarbeitung von Daten rechtmäßig, d.h. gesetzeskonform, erfolgt. Grundlagen sind z.B. die DSGVO (EU-Datenschutz-Grundverordnung), das Datenschutzgesetz (DSG) oder das Telekommunikationsgesetz (TKG).
- **Datensicherheit**: Umfasst in Bezug auf personenbezogene Daten jene Sicherheitsmaßnahmen, die den gesetzlichen Datenschutz gewährleisten, insbesondere Zutrittsschutz und Zugriffsschutz.
- **IT-Sicherheit**: Bezweckt den Schutz von elektronisch verarbeiteten Daten und der zur Datenverarbeitung verwendeten IT-Systeme.
- **Informationssicherheit**: Bezweckt den Schutz von Daten und Informationen in jeglicher Form, d.h. auf Papier, gesprochen sowie elektronisch und in sonstiger Weise verarbeitet, kurz: die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit von Daten und Informationen.
- **IT-Endgerät**: Standgeräte (Desktops), tragbare Geräte (Notebooks, Tablets etc.), netzwerkfähige Kleingeräte (Smartphones, Mobiltelefone, Navigationsgeräte, Datenerfassungsgeräte, VoIP-Telefone etc.), Endgeräte in Verbindung mit medizinisch-technischen Geräten sowie Multifunktionsgeräte (Kombifaxe, Druck- bzw. Faxstationen etc.).
- **Mobiler Datenträger**: Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten (z.B. magnetisch und flashspeicher-basiert), CDs, DVDs, Disketten, Magnetbänder und ähnliche Speichermedien.
- **BYOD** (Bring Your Own Device): Mitarbeiter/innen verwenden private Geräte für dienstliche Zwecke, z.B. um dort E-Mails zu empfangen. Erfordert die Zustimmung des Arbeitgebers.
- **Schadsoftware**: Programme, die vorsätzlich schädigende Funktionen auszuführen. Der Begriff bezeichnet also keine schadhafte, sondern vorsätzlich schädigende Software. Das kann z.B. das Löschen von Dateien sein, das Verschlüsseln von Daten und Erzwingen von Lösegeldzahlungen oder das Einnisten von Software zum Zweck des Ausspähens von Tastaturanschlägen, z.B. bei der Passworteingabe.

Welche Datensicherheitsmaßnahmen muss ich setzen?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Einige **Beispiele**:

- Setzen eines Geräte-PIN z.B. am Smartphone oder Tablet
- Verwenden eines angemessenen Passworts unter Windows
- Shredden von Papier
- Speichern von dienstlichen personenbezogenen Daten nur auf Geräten der MUI
- Verwenden von Vertraulichkeitsvereinbarungen mit Externen
- Verwenden von externen Festplatten, USB-Sticks und Speicherkarten nur mit Verschlüsselung, z.B. mit Bitlocker (unter Windows möglich) oder von Festplatten mit integrierter Verschlüsselung und Tastenfeld für eine PIN-Eingabe.
- Einstellen der automatischen Löschung aller Daten z.B. am Smartphone oder Tablet nach zehn erfolglosen Login-Versuchen
- Verschließen der Zimmertüre
- Verwenden des Zimmersafes in Hotels, z.B. für das Notebook

Details und weitere Maßnahmen finden Sie weiter hinten in diesem Foliensatz.

Außerdem finden Sie wichtige Informationen zum Umgang mit schutzbedürftigen Daten hier.

Was muss ich beachten, wenn ich öffentliche Cloud-Lösungen für dienstliche Daten verwenden möchte?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Typische **Probleme** bei öffentlichen Cloud-Lösungen:

- Datenschutzrecht – die Rechtmäßigkeit ist oft nicht gegeben
- Freigabe von Dateien und Verzeichnissen – es können ungewollt ganze Abteilungsserver geteilt und synchronisiert werden
- Sicherung – Verwechslung von Synchronisation mit Sicherung und in Folge Datenverlust

Die dienstliche Verwendung z.B. der Dropbox, der iCloud, ja der meisten US-amerikanischen öffentlichen Cloud-Angebote zur Verarbeitung schützenswerter interner oder vertraulicher, insbesondere personenbezogener Daten, ist daher in der Regel unzulässig, weil sie **nicht** der geltenden Rechtslage entspricht.

Im Zweifel kontaktieren Sie bitte die Abteilung IT oder die Rechtsabteilung.

Welche vorgesehenen Cloud-Lösungen gibt es an der MUI?

Die folgenden Cloud-Lösungen sind z.B. von der MUI für dienstliche Zwecke vorgesehen und freigegeben:

- **Nextcloud** – zur Übermittlung und zum Bearbeiten von Dateien
- **ACOnet FileSender** – zur Übermittlung von Dateien
- **Confluence** – eine Wiki-Lösung für die Dokumentation und Kommunikation von Wissen und zum Wissensaustausch
- **Webex** – eine Lösung für Webkonferenzen und Videokonferenzen
- **Academic AI** – eine spezielle, für die MUI bereitgestellte Variante von ChatGPT für hochschulische Zwecke

Weitere Informationen finden Sie hier.

Was muss ich tun, damit Unterlagen und elektronische Datenträger sicher entsorgt werden können?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Verwenden Sie für interne und vertrauliche Unterlagen auf Papier die aufgestellten Datenschutzcontainer oder Shredder – und entsorgen Sie auf diesem Weg lieber einmal ein Dokument zu viel als zu wenig.
- Haben Sie weder einen Datenschutzcontainer noch einen Shredder zur Verfügung, z.B. auf Reisen, dann zerreißen Sie interne und vertrauliche Unterlagen in kleine Stücke und entsorgen Sie das Papier im Restmüll – zusätzlicher Müll macht das Papier weiter unlesbar und Restmüll wird darüber hinaus in der Regel häufiger abgeholt als Altpapier. Oder Sie nehmen die Unterlagen wieder in Ihr Büro mit und entsorgen sie dort.
- Bringen Sie elektronische Datenträger wie USB-Sticks, CDs, DVDs etc. mit internen oder vertraulichen Daten entweder zur Abteilung IT oder zerstören sie diese selbst.

  Aber Achtung: Magnetplatten in Festplatten zum Beispiel zerspringen in viele kleine, scharfkantige Stücke und bestimmte Akku-Arten können Feuer fangen. Um Verletzungen zu vermeiden, sollten Sie diese Datenträger bevorzugt von der Abteilung IT vernichten lassen.
- Erreichen IT-Endgeräte das Ende ihrer Nutzungsdauer oder sind defekt, verwahren Sie diese sicher (idealerweise versperrt) und retournieren Sie sie ehestmöglich an die Abteilung IT.

Die Abteilung IT unterstützt Sie bei allen Fragen zu sicherer Löschung und Vernichtung von Datenträgern.

Was muss ich in Bezug auf Datensicherung beachten?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Daten auf **zentralen Systemen** werden von der Abteilung IT routinemäßig gesichert.
- Speichern Sie Ihre Daten daher grundsätzlich auf Ihrem **persönlichen zentralen Speicherbereich** oder an anderen, **zentral** gesicherten Speicherorten.
- Sollten Sie dennoch Daten **lokal** auf Ihren Geräten speichern, sichern Sie diese
  - regelmäßig auf Ihren persönlichen zentralen Speicherbereich
  - zusätzlich, wenn Sie umfangreiche Änderungen an lokalen Daten vorgenommen haben
  - nachdem Sie aufwendig z.B. neue Dokumente, Tabellen etc. erstellt haben und
  - in jedem Fall bevor Sie verreisen, egal ob dienstlich oder urlaubsbedingt.
- Sollten Sie mit einem Notebook oder Tablet PC unterwegs sein, können Sie sich Dokumente zur Sicherung auch z.B. per E-Mail selbst schicken, wodurch sie auf zentralen Systemen gesichert werden.

Sichern Sie dienstliche Daten, insbesondere schützenswerte, auf keinen Fall unverschlüsselt auf mobilen Datenträgern, z.B. auf USB-Sticks, Speicherkarten oder externen Festplatten. Der richtige Ort dafür sind die zentralen Systeme der MUI.

Was muss ich bei der E-Mail-Nutzung beachten?

Die MUI erlaubt Ihnen eine eingeschränkte private Nutzung Ihrer dienstlichen E-Mail-Adresse.

Seien Sie sich bewusst, dass über die so genannte IP-Adresse jede Verwendung von E-Mail auf die MUI rückgeführt werden kann, Sie also indirekt immer im Namen der MUI agieren.

Wesentliche Regelungen lauten:

- Keine Verwendung der dienstlichen E-Mail-Adresse für z.B. politische oder aktivistische Zwecke
- Keine Vermittlung des Eindrucks, Sie handelten im Namen oder Auftrag der MUI, wenn Sie die dienstliche E-Mail-Adresse privat verwenden

Nach österreichischer Rechtslage dürfen E-Mails zu Aussendungs- und Werbezwecken nur dann versendet werden, wenn vorher eine entsprechende Zustimmung der Empfänger eingeholt worden ist. Das betrifft z.B. neben klassischen Newslettern auch Veranstaltungseinladungen, Gewinnspiele, Zufriedenheitsumfragen und Aussendungen.

Beachten Sie auch die Informationen hier.

Hilfreiche Tipps zum Schutz vor Betrug im Zusammenhang mit E-Mail finden Sie z.B. auch auf der Watchlist Internet. Zusätzliche, wichtige Informationen betreffend Massenaussendungen finden sich bei der WKO.

Was muss ich bei der Internet-Nutzung beachten?

Die MUI erlaubt Ihnen eine eingeschränkte private Nutzung Ihres Internet-Zugangs. Alle untenstehenden Regelungen beziehen sich auf beide Formen der Nutzung, dienstlich und privat.

Seien Sie sich bewusst, dass über die so genannte IP-Adresse jeder Zugriff in das Internet auf die MUI verweist, Sie also indirekt auch immer im Namen der MUI agieren.

Beachten Sie besonders die Informationen hier.

Wesentliche sicherheitsbezogene Maßnahmen sind z.B. die folgenden:

- Der Sperrbildschirm auf Notebooks bzw. Desktops ist so einzustellen, dass er spätestens nach 10 Minuten Inaktivität aktiviert wird und ist bei Verlassen des Arbeitsplatzes manuell zu aktivieren.
- Urheberrechte sind zu wahren und Lizenzbestimmungen sind einzuhalten.

Bedenken Sie, dass die private Internet-Nutzung insbesondere rechtlich eine Vielzahl von Fragen aufwirft und reduzieren Sie diese bitte auf ein Minimum.

Hilfreiche Tipps zum Schutz vor Online-Betrug und vor Fallen finden Sie z.B. auch auf der Watchlist Internet.

Wie mache ich meinen Arbeitsplatz sicherer?

- Stellen Sie sicher, dass in Ihrem Arbeitsbereich Unterlagen und Datenträger, z.B. USB-Sticks, mit internen oder vertraulichen Informationen nicht durch Unberechtigte einsehbar abgelegt sind – räumen Sie interne und vertrauliche Unterlagen, jegliche Datenträger sowie mobile IT-Endgeräte bei Abwesenheit in einen Kasten oder eine Lade und versperren Sie diese, sofern möglich.
- Sollte z.B. Reinigungspersonal Ihren Arbeitsbereich üblicherweise unbeaufsichtigt betreten können, müssen Sie zu diesen Zeiten schutzbedürftige Unterlagen, Datenträger und IT-Endgeräte auf jeden Fall zugriffsgeschützt lagern.
- Verwenden sie ein Kabelschloss, wenn Sie ein Notebook besitzen.
- "Sperren" Sie Ihren PC bzw. ihr Notebook, sowohl wenn Sie Ihren Arbeitsplatz kurzfristig, besonders aber für längere Zeit verlassen, mit der Tastenkombination **Windows-Taste+L** und lassen Sie Smartphones, Tablets etc. nicht unversperrt, d.h. ohne PIN bzw. Passwort im Raum liegen.
- Beachten Sie auch die weiteren sicherheitsbezogenen Regelungen der MUI.

Denken Sie daran, dass Sie gemäß DSGVO und DSG verpflichtet sind, Unterlagen und Datenträger vor unberechtigtem Zugriff zu schützen. Das betrifft auch Notebooks, Smartphones, Tablets etc., die häufig von Betriebsfremden, manchmal leider aber auch „Insidern“, gestohlen werden.

Wie gehe ich mit mobilen Datenträgern um?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Mobile Datenträger sind z.B. Speichersticks (USB-Sticks), Speicherkarten aller Art (auch in Multimedia-Abspielgeräten, in Kameras etc.), mobile Festplatten, DVDs und ähnliche Speichermedien.
- Stecken Sie keine gefundenen USB-Sticks an, ebensowenig solche, die Sie auf Messen, Konferenzen etc. bekommen – sie sind **der** Weg, über den Schadsoftware ohne Netzwerkverbindung in Unternehmen gelangt.
- Fragen Sie sich, ob Sie externe Datenträger wie USB-Sticks überhaupt benötigen und nicht andere Wege wie z.B. E-Mail, Nextcloud oder ACOnet FileSender besser geeignet sind.
- Sollten Sie mobile Datenträger entsorgen müssen oder wollen, so geben Sie diese bitte bei der Abteilung IT ab, wo sie zerstört werden. Sollten mobile Datenträger unverschlüsselte, schützenswerte Daten beinhalten, z.B. vertrauliche oder personenbezogene Daten, so muss der mobile Datenträger auf jeden Fall bei Abteilung IT abgegeben bzw. von Ihnen selbst verlässlich zerstört werden, beispielsweise durch Lochung von DVDs oder Zertrümmern eines USB-Sticks – Achtung jedoch: Splittergefahr!

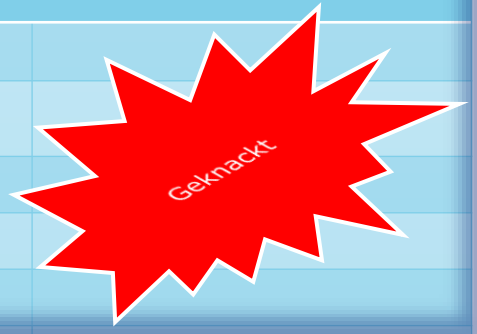
Mobile Datenträger sind eines der größten Einfallstore für Schadsoftware.
Sie stellen eine potenzielle Schwachstelle dar, was den Verlust der Vertraulichkeit sensibler Daten betrifft.

„Knackdauer“ bei Passwörtern

Rechengeschwindigkeit des Computers: rund zwei Milliarden Varianten pro Sekunde

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Passwortlänge	„Knackdauer“	Einheit	Anmerkung
a-z, A-Z, 0-9 (= 3 Merkmale)	maximal		
6	27	Sekunden	
7	28	Minuten	
8	29	Stunden	
9	75	Tage	
10	12	Jahre	
11	**787**	**Jahre**	
12	**48.804**	**Jahre**	
13	**3.025.880**	**Jahre**	**> 3 Millionen Jahre**
14	**187.604.571**	**Jahre**	**> 187 Millionen Jahre**
15	**11.631.483.455**	**Jahre**	**> 11 Milliarden Jahre**



„Tipps“ für *wirkungslose* Passwörter…

In der Praxis **unsichere** Passwörter sind beispielsweise

- kurz, z.B. weniger als 10 bis 12 Zeichen lang – außer es sind PINs, wie z.B. auf SIM-Karten, die nach wenigen Fehlversuchen gesperrt werden
- einfache Wörter und Namen, z.B. Häschen, Passwort, Hans, Marie
- schlicht aufgebaut, z.B. 0000, 123456, abcfeghi, qwertzuio (Tasten nebeneinander)
- ident mit Wörtern aus Wörterbüchern

Erfolgreiches „Passwort-cracken“ ist damit ein Kinderspiel

Wie aber sehen sichere, wirksame Passwörter aus?

Tipps für sichere, recht leicht merkbare Passwörter

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Erzeugen Sie **lange** Passwörter – das macht alles einfacher:
  10 Zeichen sind das Minimum, 12 bis 16 Zeichen sind empfehlenswert.
  Aber Achtung: Manche IT-Systeme oder Programme erlauben keine Passwörter länger als 8 oder 15 Zeichen.
- Denken Sie **bildlich**
- Verwenden Sie **Groß- und Kleinbuchstaben**, **Ziffern und Sonderzeichen**
  Bin1Schon2Da3 – &waa7ruum? – DerWurmIm%Sturm
- **Reihen** Sie Wörter aneinander oder **teilen** Sie sie
  2Und2istVier? – Uff!Zack!Knuff! – Per1Se2Polis3
- **Reimen** Sie
  3Motten&5Karotten – Elch&Kelch1 – Heute!ister!beute! – EinBIER-um4
- Verwenden Sie **Dreiergruppen** aus Buchstaben in Kombination mit Ziffern, das ist eingängiger
  &Aaa4Bee5Cee – Nic9Jul8Ras7
- Warum nicht **Dialekt?**
  SchneeIschSchee! – 25IsaguatsJoa – Aquartal.is.a.Qual – MeiPWIsSchee!

Schlechter Umgang mit Passwörtern und PINs sieht so aus…

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Passwörter werden beispielsweise **leichtfertigerweise**

- **bei verschiedenen Diensten mehrfach genutzt („eines für alles“)**
- auf Zetteln gut zugänglich notiert
- auf PCs, Notebooks, Smartphones etc. unverschlüsselt gespeichert
- mit anderen geteilt
- vor anderen mitlesbar eingeben („shoulder surfing“ wird ermöglicht)
- sehr selten oder nie geändert
- über E-Mail verschickt
- im Browser abgespeichert
- auf fragwürdigen Seiten oder in zweifelhafte Apps eingegeben

Identitätsdiebstahl steht nun nichts mehr im Weg

Wie aber sieht guter Umgang mit Passwörtern aus?

Vernünftiger Umgang mit Passwörtern und PINs hingegen sieht folgendermaßen aus

Passwörter – dienstliche, sinnvollerweise aber auch private – werden

- geheim gehalten – das gilt gegenüber allen Personen, auch Familienmitgliedern und Partnern
- wenn überhaupt, nur an schwer zugänglichen, anderen Personen unbekannten Orten notiert
- auf PCs, Notebooks, Smartphones etc. nur verschlüsselt gespeichert – im Zweifel allerdings überhaupt nicht
- geändert, wenn andere sie gesehen haben oder kennen könnten
- regelmäßig geändert, und sei es auch nach längerer Zeit
- niemals bei anderen Diensten wiederholt genutzt („eines pro Dienst“)
- nie über E-Mail verschickt
- nie im Browser abgespeichert
- nie auf fragwürdigen Seiten oder in zweifelhafte Apps eingegeben

Bitte beachten Sie die Passwortregelungen hier

Was ist Phishing und wie schütze ich mich davor?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Phishing ist ein Variante des „Social Engineering“, der zwischenmenschlichen Beeinflussung für unlautere Zwecke – oft für Identitätsdiebstahl.
- Klicken Sie Links in Spam-E-Mails niemals an und löschen Sie derartige Nachrichten umgehend, und zwar auch aus Ihrem „Papierkorb“ – am besten sofort mit der Windows-Taschenkombination **Umschalt+Entf**.
- Misstrauen Sie dringend erscheinenden E-Mails, die von Ihnen unter Zeitdruck persönliche Daten und/oder Zugangsdaten, auch PINs und TANs abfragen möchten, z.B. indem Ihnen mit der Sperre von Zugängen gedroht wird.
- Reagieren Sie nicht auf E-Mails, in denen, unter welchem Vorwand auch immer, auf verlinkten Webseiten die Eingabe von Zugangsdaten gefordert wird. Dasselbe gilt auch für Apps, die angeblich aufhören zu funktionieren, wenn Sie nicht einen speziellen Link anklicken.
- Geben Sie Zugangsdaten nie über unsichere Internetverbindungen ein, d.h. *keinesfalls* über „http“-Webseiten, sondern nur über solche, die mit „http**s**“ beginnen.
- Auch betreffend Telefonie gilt: Übermitteln Sie keine vertraulichen Daten (Benutzernamen, Passwörter, TANs etc.), ausgenommen Sie sind sicher, dass der/die Empfänger:in vertrauenswürdig ist. Ein Beispiel: Sie haben Ihre Bank oder Ihren Internet-Provider selbst unter der Ihnen bekannten Service-Telefonnummer angerufen: Dann ist das die sicherste Form der Kontaktherstellung.

Weitere Praxistipps zum Schutz vor Passwort-Fishing (Phishing) finden Sie z.B. auf der Watchlist Internet und im IT-Sicherheitshandbuch für Mitarbeiter/innen der WKO ab Seite 26.

Ransomware (Erpressungstrojaner) und wie ich mich vor ihnen schütze

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Erpressungstrojaner sind eine besondere Form von Schadsoftware, d.h. von Computerprogrammen, die vorsätzlich schädigende Funktionen auszuführen. Der Begriff bezeichnet also keine schadhafte, sondern gewollt schädigende Software.
- Erpressungstrojaner, auch Lösegeldtrojaner, Verschlüsselungstrojaner und „Ransomware“ (Erpressungs-Software) genannt, verschlüsseln in der Regel alle Dokumente, Tabellen, Präsentationen, Fotos, Musikdateien und sonstigen Nutzerdaten, auf die diese Software Zugriff erlangt. Gegen Bezahlung eines Lösegelds an die organisierte Kriminalität werden diese Dateien – zumeist – wieder entschlüsselt.
- Eintrittswege für diese Form der Schadsoftware sind in der Regel
  - E-Mail-Anhänge, z.B. scheinbare Rechnungen, Paketankündigungen oder Bewerbungen und
  - von den Kriminellen verseuchte oder präparierte Webseiten, die Sicherheitsschwachstellen auf schlecht gepflegten IT-Systemen der Nutzer ausnützen.
- Der wesentlichste Schutz vor derartiger Erpressung ist das Sichern von Daten auf den zentral gesicherten Speicherbereichen der MUI und der vorsichtige Umgang mit erhaltenen Dateien, z.B. Dokumenten und Tabellen.
- **Sollten Sie feststellen, dass Sie Opfer einer Erpressung in Kombination mit Verschlüsselung geworden sind, kontaktieren Sie bitte umgehend den Helpdesk unter helpdesk@i-med.ac.at**
- Leisten Sie keinesfalls Zahlungen.

Für Details und aktuelle Beispiele von im Umlauf befindlichen Erpressungstrojanern und für Schutzmaßnahmen und Tipps werfen Sie bitte einen Blick auf die äußerst hilfreiche Seite der Watchlist Internet.

Was ist Schadsoftware?

- Schadsoftware bezeichnet Programme bzw. Apps, die vorsätzlich schädigende Funktionen auszuführen.
- Der Begriff bezeichnet also keine schadhafte, sondern gewollt schädigende Software.
- Das kann z.B. das Löschen von Dateien sein, das Verschlüsseln von Daten und Erzwingen von Lösegeldzahlungen oder das Einnisten von Software zum Zweck des Ausspähens von Tastaturanschlägen, z.B. bei der Passworteingabe.
- Die wesentlichsten Schutzmaßnahmen werden von der Abteilung IT gesetzt.

Für Details und aktuelle Beispiele von im Umlauf befindlichen Erpressungstrojanern und für Schutzmaßnahmen und Tipps werfen Sie bitte einen Blick auf die äußerst hilfreiche Seite der Watchlist Internet.

Wie schütze ich mich vor Schadsoftware?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Sie als Mitarbeiter:in haben es in der Hand, jene Angriffe abzuwehren, die **technisch** nicht verhinderbar sind:

- Sichern sie wichtige Daten auf zentrale Systeme.
- Misstrauen Sie E-Mail-Anhängen grundsätzlich und fragen Sie bei Unsicherheit beim Absender nach, bevor Sie die Datei im Anhang öffnen.
- Halten sie den Schadsoftwareschutz aktuell, insbesondere unter Windows, und lassen Sie, wenn Sie länger nicht an Ihrem IT-Endgerät gearbeitet haben, den Schadsoftwarescanner erst einmal Updates herunterladen und installieren – 5 bis 10 Minuten reichen dafür aus.
- Ermöglichen Sie dem Betriebssystem, insbesondere Windows, automatisch Sicherheitsupdates herunterzuladen und zu installieren, v.a. wenn Sie lange nicht an Ihrem IT-Endgerät gearbeitet haben – 10 bis 15 Minuten reichen dafür meist aus.
- Vermeiden Sie es, mit so genannten Administratorrechten zu arbeiten (sofern Sie dazu überhaupt die Möglichkeit haben).
- **Melden Sie ungewöhnliches Verhalten Ihrer IT-Endgeräte so rasch wie möglich an helpdesk@i-med.ac.at**

Was ist Social Engineering?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Social Engineering ist die Kunst, Menschen dahingehend zu beeinflussen, dass sie bestimmte Verhaltensweisen setzen, selbst wenn diese nicht in ihrem Interesse liegen. Z.B. könnte sich jemand Zutritt zu einem Gebäude verschaffen, indem er, gut gekleidet und selbstbewusst, eine sich schließende Tür noch schnell aufdrückt und sich, dem vor ihm Eingetretenen dankend, zügig Zutritt zu einem Bereich verschafft, der eigentlich nur Personen mit Zutrittskarte offensteht.
- Social Engineering stellt einen Angriff auf menschliches Verhalten dar und kann als eine Form von Hacking gesehen werden.
- Die Schwachstelle bei Social Engineering ist der Mensch, nicht die Technik.
- In der Regel dient Social Engineering missbräuchlichen Zwecken wie Daten- und Identitätsdiebstahl, Spionage und Betrug.
- Zu den Methoden von Social Engineering gehören gezieltes Aushorchen von Mitarbeiter/inne/n, widerrechtliches Abfragen oder Abfangen von Passwörtern, das unerlaubte Erwirken von Zutritt zu Gebäuden und Büros etc.
- Angreifer spionieren das persönliche Umfeld ihres Opfers aus, spiegeln falsche Identitäten vor oder nutzen Schwächen wie Autoritätshörigkeit.
- Es wird tief in die Trickkiste der Psychologie gegriffen, per Telefon, Brief, Fax, E-Mail, über Social Media, persönliches Ansprechen und weitere Wege.

In welche psychologische Trickkiste greifen „Social Engineers“ beispielsweise?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Datendiebe, Kriminelle und andere Unredliche adressieren gerne…

- Liebe
- Vertrauen
- Neugierde
- Hilfsbereitschaft
- Risikofreude

- Abenteuerlust
- Geltungsdrang und Geltungssucht
- Geschwätzigkeit

- Naivität
- Sorglosigkeit
- Stressanfälligkeit
- Bequemlichkeit
- Autoritätsglaube
- Überzeugungen

- Schreck und Blockade
- Sorge um Verknappung
- Angst vor Verlust
- Frustration
- Schuldgefühle
- Schamgefühle
- Vergesslichkeit

- Zorn
- Hass
- Kompensationsbedürfnis
- Rachegelüste
- Habgier, Raffgier

- Sensorische Überforderung, v.a. Konzentrationsunfähigkeit
- Kleine Fehltritte
- Straffälligkeit
- Geldnot, Schulden

Praxistipps zum Schutz vor Social Engineering über E-Mail, Fax und am Arbeitsplatz

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Sie bekommen ein E-Mail oder Fax, das Sie unsicher macht oder begegnen im Bürobereich jemanden, der etwas zu suchen scheint, ziellos wirkt oder sogar ganz besonders forsch auftritt?

Seien Sie selbstbewusst und bestimmt.
Sie machen damit genau das Richtige.

- Lassen Sie sich nicht unter Druck setzen, versuchen Sie, Zeit zu gewinnen – sagen Sie „Lassen Sie uns zum Sekretariat gehen“ oder sprechen Sie mit Kollegen über das seltsame E-Mail, das Sie gerade erhalten haben.
- Leiten Sie E-Mails/Chat-Nachrichten und Faxe umgehend zur Prüfung an die Abteilung IT weiter.
- Begleiten Sie Personen, die behaupten sich verlaufen zu haben, zum Ausgang.
- Seien Sie hilfsbereit – und dennoch vorsichtig. Hier liegt Ihre größte Schwachstelle.
- Geben Sie beim leisesten Zweifel oder kleinstem unangenehmen Gefühl keinerlei Informationen oder personenbezogene Daten preis – weder über sich noch über andere.
- Tätigen Sie größere Zahlungen, sofern dies zu Ihren dienstlichen Aufgaben gehört, nur nach dem Vier-Augen-Prinzip.
- Melden Sie Ungewöhnliches lieber einmal zu viel als zu wenig – und dies rasch.

Praxistipps zum Schutz vor Social Engineering über Telefon und im Gespräch

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

Sie bekommen einen Anruf oder werden persönlich angesprochen? Man will Auskünfte, ist seltsam neugierig oder schmeichelt Ihnen? Sie fühlen sich daher unwohl?

Seien Sie zurückhaltend und fragen Sie zurück.
Sie machen damit genau das Richtige.

- Lassen Sie sich nicht unter Druck setzen, versuchen Sie, Zeit zu gewinnen – sagen Sie „Einen Moment bitte, es läutet gerade“ oder „Moment, ich bin gleich wieder bei Ihnen“.
- Fragen Sie zurück und bitten Sie um Kontaktdaten. Sagen Sie beispielsweise, Sie seien nicht zuständig und benötigten daher diese Daten.
- Bitten Sie am Telefon freundlich um eine Rückrufnummer. Sagen Sie, Sie müssten dies tun und halten Sie nach dem Gespräch rasch Rücksprache mit Ihrem Vorgesetzten oder melden Sie den Vorfall.
- Bei (angeblichen) Anrufen durch die Presse sagen Sie, sie seien nicht auskunftsberechtigt und verweisen Sie an das Rektorat. Verständigen Sie ehestmöglich die von Ihnen genannte Stelle über allfällige Bedenken Ihrerseits.
- Melden Sie ungewöhnliche Anrufe und Gespräche lieber einmal zu viel als zu wenig.

Wie verhalte ich mich in der Öffentlichkeit, um interne und vertrauliche Informationen zu schützen?

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Führen Sie keine vertraulichen dienstlichen Gespräche beispielsweise in öffentlichen Verkehrsmitteln wie Bussen, Straßenbahnen oder Flugzeugen, am Mittagstisch am Campus, bei externen Veranstaltungen etc., außer Sie haben sich vorab überzeugt, dass niemand Unbefugter Sie hören oder Unterlagen einsehen kann. Das gilt auch für Telefonate.
- Benützen Sie ein Notebook, Tablet oder Smartphone nur dann, wenn Sie sich überzeugt haben, dass niemand Unbefugter Ihren Bildschirm einsehen kann.
- Stellen Sie die Dauer für die Aktivierung der Gerätesperre so kurz wie möglich ein, z.B. am Smartphone auf eine oder zwei Minuten und auf Aktivierung beim Drücken des Ein-Aus-Schalters.
- In Flugzeugen, je nach Sitzanordnung auch in der Bahn, sollten Sie Notebooks nicht verwenden, da es so gut wie immer Menschen gibt, die mitlesen können. Dort hilft selbst eine spezielle Datenschutzfolie, die seitliches Mitlesen verhindert, nur selten.
- Vermeiden Sie, wann immer möglich, die Erwähnung von Nachnamen von Personen und Namen von Firmen, Behörden, anderen Universitäten etc.
- Bedenken Sie, dass Schall manchmal überraschende Wege finden kann, um sich zu verbreiten und dass auch im Ausland Menschen oftmals Deutsch verstehen, von denen man das nicht erwarten würde. Wer z.B. eine nicht-deutschsprachige Zeitung liest, kann dennoch z.B. Tourist und muttersprachlich deutschsprachig sein.

Tipps für unterwegs – z.B. im Auto, im Bus, in der U-Bahn und Straßenbahn

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Was nicht mitgenommen wird, kann nicht gestohlen werden.
- Muss Papier wirklich mit, wenn es vertrauliche Daten enthält?
- Für das Notebook eine neutrale Tasche verwenden.
- USB-Sticks nur mitnehmen, wenn vertrauliche Daten darauf verschlüsselt sind.
- Das Auto ist kein Safe – Geräte, Taschen etc. nie sichtbar darin liegen lassen.
- Geräte wie Smartphones, Tablets und Notebooks nie unbeaufsichtigt liegen lassen, nicht im Meetingraum, nicht im Lokal, nicht für einen Toilettenbesuch.
- Bei Veranstaltungen in den Pausen ein Kabelschloss verwenden – bei den meisten „Business“-Notebooks ist das problemlos möglich.

Auf Reisen mit IT – Tipps für Dienstreisen und Urlaube

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Was nicht mitgenommen wird, kann weder gestohlen werden noch verloren gehen.
- Wertsachen, also auch Smartphones und Tablets, nicht mit Kleingepäck, v.a. nicht in Außentaschen, aufgeben.
- Geräte wie Smartphones und Notebooks nie unbeaufsichtigt liegen lassen – nicht im Zug, nicht im Café, nicht für einen Toilettenbesuch.
- Das Auto ist kein Safe – Geräte, Taschen etc. darin nie sichtbar liegen lassen.
- Ein Kabelschloss verwenden – bei den meisten „Business“-Notebooks problemlos möglich.
- Den Zimmersafe verwenden. Kein Safe vorhanden? Dann in den Koffer legen und dort versperren – vorausgesetzt, man hat ein Schloss eingepackt. Im Idealfall ist es im Koffer integriert.
- Den MUI VPN-Zugang wann immer möglich verwenden – die gesamte Kommunikation wird dadurch verschlüsselt und geschützt.
- Hotel-WLANs und andere öffentliche WLANs wenn möglich vermeiden – sofern Roaming ohne Zusatzkosten möglich ist.
- Zugangsdaten nie auf fragwürdigen Geräten eingeben, etwa auf fremden Privatgeräten, auf Hotelgeräten oder in Internet-Cafés.
- Daten, die z.B. lokal am Notebook liegen, vor der Reise sichern.

Sicher im Home Office und bei Telearbeit

MEDIZINISCHE UNIVERSITÄT INNSBRUCK

- Geräte-PINs bzw. Login-Passwörter verwenden
- Passwörter nicht sichtbar notieren
- Bei z.B. Webex-Konferenzen: Vorsicht bei der Bildschirmfreigabe
- USB-Sticks und Speicherkarten nicht zur Ablage von internen oder vertraulichen Informationen verwenden
- Zu entsorgende Unterlagen und Datenträger an die MUI mitnehmen
- Unterlagen zumindest nach Arbeitsende wegräumen: Kasten, Lade, als Stapel mit neutralem Deckblatt

Was tue ich bei Sicherheitsvorfällen und wenn ich Sicherheitsmängel vermute oder entdecke?

Zögern Sie bitte nicht, Vorfälle oder Mängel zu melden: Es geht der MUI nicht darum, Schuldfragen zu klären, sondern Schäden durch Sicherheitsvorfälle und -mängel zu minimieren und zukünftig auszuschließen.

Meldung von sicherheitsrelevanten Vorfällen oder Sicherheitsmängeln allgemein:

- helpdesk@i-med.ac.at

Meldung *kritischer* sicherheitsrelevanter Vorfälle, insbesondere von Vorfällen mit möglicher Öffentlichkeitswirksamkeit (Datenverlust, Datendiebstahl, Cyberangriffe etc.):

- helpdesk@i-med.ac.at und **zusätzlich** Meldung an die vorgesetzte Führungskraft, um die weiteren Schritte einzuleiten.

Löschen Sie nach der Meldung weder E-Mails noch andere Daten und verwenden Sie die betroffenen Geräte nicht weiter.

Eine Pflicht zur **umgehenden** Meldung besteht beispielsweise

- bei Verlust oder Diebstahl von Unterlagen oder von IT-Endgeräten, z.B. von Smartphones, Tablets oder Notebooks, oder von Datenträgern wie z.B. unverschlüsselten USB-Sticks
- bei Auftreten von Schadsoftware oder seltsamem Geräteverhalten, z.B. plötzlichen Systemabstürzen, eigenartigen Fehlermeldungen, Mitteilungen über angebliche Vergehen
- bei ungewöhnlichen E-Mails oder Anrufen, insbesondere, wenn dabei nach Passwörtern oder Informationen über Kollegen gefragt wird
- bei Auftreten von ungewollter Datenverschlüsselung, verbunden mit Zahlungsaufforderungen – sogenannten Erpressungstrojanern

Melden Sie sicherheitsrelevante Vorfälle und Sicherheitsmängel im Zusammenhang mit IT umgehend – große Schäden in anderen Organisationen hätten verhindert werden können, wären Vorfälle oder Auffälligkeiten rasch gemeldet worden.

Aktuell geltende Regelungen und Empfehlungen

Die Regelungen der MUI zu Informationssicherheit finden Sie hier:

- Informationssicherheit an der MUI

Datenschutzrelevante Informationen finden Sie hier:

- Datenschutzkoordination (Intranet der MUI)

Externe Sicherheitstipps finden Sie z.B. hier:

- IT-Sicherheitshandbuch für Mitarbeiter/innen (WKO)

Damit es zu so wenig Sicherheitsvorfällen wie möglich kommt, bietet die Abteilung IT zahlreiche Empfehlungen, die auch für Ihre IT-Nutzung im Privatleben hilfreich sein können.

Kontaktinformationen

Meldung von sicherheitsrelevanten Vorfällen oder Sicherheitsmängeln allgemein:

- helpdesk@i-med.ac.at

Meldung kritischer sicherheitsrelevanter Vorfälle, insbesondere von Vorfällen mit möglicher Öffentlichkeitswirksamkeit (Datenverlust, Datendiebstahl, Cyberangriffe etc.):

- helpdesk@i-med.ac.at und **zusätzlich** Meldung an die vorgesetzte Führungskraft, um die weiteren Schritte einzuleiten.

Spezielle Fragen ohne Dringlichkeit:

- Datenschutz: Datenschutzbeauftragter: datenschutzkoordinator@i-med.ac.at
- Informations- und IT-Sicherheit: helpdesk@i-med.ac.at