KNYRIM.TRIEB
RECHTSANWÄLTE

DATENSCHUTZRECHT
IT-RECHT
ARBEITSVERFASSUNGSRECHT
VERTRAGSRECHT

Experten-Kanzlei für die Themen,
die Unternehmen im 21. Jahrhundert bewegen

Mitarbeiterschulung Datenschutzrecht Ecco/IBDIM

21. Dezember 2021

RA Dr. Rainer Knyrim
Knyrim Trieb Rechtsanwälte OG
Mariahilfer Straße 89A
1060 Wien

Inhalt

I. Einführung

- Bei Verstößen gegen die Bestimmungen der DSGVO drohen **hohen Geldbußen**
- **Mehr Eigenverantwortung der datenverarbeitenden Person/Stelle**
- **Verringerte Kontrolle durch die Datenschutzbehörde**
- Verlagerung der Verantwortung zum **Verantwortlichen** im Sinne eines „**risikobasierten Ansatzes**“

II. Grundbegriffe und Prinzipien

Personenbezogene Daten (Art. 4 Z 1 DSGVO):

- Daten / Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Personen beziehen
- Verarbeitung personenbezogener Daten verboten, wenn nicht ausdrücklich erlaubt
- z.B. Name, Geburtsdatum, Adresse, Telefonnummer, Fotos, Videoaufnahmen, E-Mail-Adresse, Kundennummer, KFZ-Kennzeichen, Kontonummer, Krankenstandstage, IP-Adresse, Fingerabdruck, Aussagen über physische, physiologische, genetische, psychische, wirtschaftliche, kulturelle oder soziale Eigenschaften

II. Grundbegriffe und Prinzipien

Besondere Kategorien von Daten (Art. 9 DSGVO, „sensible Daten“):

- Daten aus denen die ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen hervorgehen
- Gesundheitsdaten
- Biometrische Daten
- Daten zum Sexualleben/zur sexuellen Orientierung

II. Grundbegriffe und Prinzipien

Rollenverteilung:

- **Verantwortlicher**

  Entscheidet alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogen Daten (natürliche oder juristische Person, Behörde, Organisation, „sonstige Stelle“)

  > zahlreiche Pflichten

- **Betroffene Person**

  natürliche Person, auf die sich die Verarbeitung pbD bezieht;
  > umfangreiche Betroffenenrechte

- **Empfänger**

  Auftragsverarbeiter und Dritte, denen personenbezogene Daten offengelegt werden

II. Grundbegriffe und Prinzipien

Rollenverteilung:

- **Auftragsverarbeiter (Art. 4 Z 8 DSGVO):**
  - natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
  - Der Verantwortliche muss mit dem Auftragsverarbeiter eine Auftragsverarbeitervereinbarung abschließen
  - Achtung auf Subauftragsverarbeiter, insbesondere, wenn diese außerhalb der EU sind oder von dort kommen – zusätzliche Voraussetzung sind dann erforderlich!

II. Grundbegriffe und Prinzipien

Die wichtigsten datenschutzrechtlichen Prinzipien sind:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“,
- „Zweckbindung“
- „Datenminimierung“
- „Speicherbegrenzung“
- „Integrität und Vertraulichkeit“
  - (Schutz gegen unbefugten bzw. unrechtmäßigen Zugriff und versehentlichen Datenverlust, Zerstörung oder Schädigung durch angemessene technische oder organisatorische Maßnahmen)

Verantwortlicher ist für die Einhaltung der Grundsätze verantwortlich (Rechenschaftspflicht)!

Exkurs - Sanktionen (Art 83 DSGVO)

1 Strafrahmen bis EUR 10 Mio (2 % des weltweiten Jahresumsatzes)

- Verstoß gegen Bestimmungen zu Datenschutz durch Technik (privacy by design);
- Verstoß gegen Bestimmungen zur Auftragsdatenverarbeitung;
- Verletzung der Vorschriften zum „Verzeichnis von Verarbeitungstätigkeiten“;
- Verletzung von Datensicherheitsbestimmungen / Datenschutzfolgenabschätzung;

→ **„Verletzung von Pflichten der Verantwortlichen“**

Strafrahmen bis EUR 20 Mio (4 % des weltweiten Jahresumsatzes) 2

- Verletzung von Rechten betroffener Personen;
- Verletzung von Bestimmungen über den internationalen Datenverkehr;
- Verstoß gegen Bestimmungen gegen die Grundsätze rechtmäßiger Datenverarbeitung;

→ **„Verletzung von Rechten betroffener Personen“**

III. Zulässigkeit der Datenverarbeitung (Art 6 DSGVO)

- **Einwilligung** (Art 6 Abs 1 lit a DSGVO)
- **Vertragserfüllung** oder **Durchführung vorvertraglicher Maßnahmen**, die auf Anfrage des Betroffenen erfolgen (Art 6 Abs 1 lit b DSGVO)

  z.B. Vertragsabwicklung mit Geschäftspartnern und Kunden, Lohnverrechnung, Bewerberdaten
- **Erfüllung einer rechtlichen Verpflichtung** (Art 6 Abs 1 lit c DSGVO)

  z.B. steuerrechtliche und unternehmensrechtliche Aufbewahrungs- und Dokumentationspflichten, Geldwäschebestimmungen
- **Lebenswichtige Interessen des Betroffenen oder eines Dritten** (Art 6 Abs 1 lit d DSGVO)
- Wahrnehmung einer **Aufgabe im öffentlichen Interesse** oder in **Ausübung öffentlicher Gewalt**, die Verantwortlichem übertragen wurde (Art 6 Abs 1 lit e DSGVO)
- **Berechtigte Interessen des Verantwortlichen oder eines Dritten** (Art 6 Abs 1 lit f DSGVO) z.B. Marketing (Achtung: § 107 Telekommunikationsgesetz 2003!)

III. Einwilligung (Art 4, Art 7 und Art 8 DSGVO)

- **Anforderungen an Einwilligungen**
  - freiwillig,
  - für bestimmten Fall,
  - informiert,
  - unmissverständlich.

Einwilligung kann jederzeit widerrufen werden!

- **Kopplungsverbot!**
- Zustimmung kann schriftlich, elektronisch (etwa: Anklicken einer Checkbox) oder mündlich erfolgen
- Achtung: **Nachweispflicht! (Rechenschaftspflicht)**

Schweigen, vorab angeklickte Checkboxen oder Untätigkeit der betroffenen Personen ist keine gültige Einwilligung!

III. Datensicherheit

- Datenschutzrecht bedeutet auch, dass die Daten technisch und organisatorisch geschützt werden. In diesem Zusammenhang spricht man von Datensicherheit. Datensicherheit ist damit eine Grundvoraussetzung für Datenschutz.

- Für die Datensicherheit sind folgende Prinzipien entscheidend:
  - **Vertraulichkeit**: Daten dürfen nur von autorisierten Benutzern gelesen bzw. modifiziert werden
  - **Integrität**: Daten dürfen nicht unbemerkt verändert werden

- § 54 DSG – Datensicherheitsmaßnahmen

Exkurs - Datengeheimnis – § 6 DSG (!)

- **Datengeheimnis**

  Verantwortliche, Auftragsverarbeiter und ihre Mitarbeiter haben personenbezogene Daten aus Datenverarbeitungen, die ihnen ausschließlich auf Grund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich gemacht worden sind, geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung besteht

- **Übermittlung von personenbezogenen Daten nur nach ausdrücklicher Anordnung durch Arbeit- bzw. Dienstgeber**

- **Vertragliche Verpflichtung der Mitarbeiter**

  Zur Datenübermittlung ausschließlich nach Anordnung durch den Arbeit- bzw. Dienstgeber und Einhaltung des Datengeheimnisses auch nach Beendigung des Arbeits- bzw. Dienstverhältnisses

Bei Verstoß gegen das Datengeheimnis droht eine Verwaltungsstrafe in Höhe von bis zu EUR 50.000!

III. Datensicherheit - „Data Breach (Datenschutzverletzung)

- **Verletzung des Schutz personenbezogener Daten**
- Beispiele
  - USB-Stick, Laptop oder Diensthandy wurde gestohlen/verloren
  - Aktentasche im Taxi vergessen
  - E-Mail an falschen Verteiler geschickt
  - Falscher Anhang im E-Mail
  - PC wurde gehackt
  - Papier entsorgt ohne zu „schreddern“
- Sofort den Vorgesetzten informieren und lückenlos Sachverhalt schildern! Die Meldung an die Datenschutzbehörde obliegt dem Datenschutzbeauftragten!

Achtung: Meldung an Datenschutzbehörde muss unverzüglich, spätestens binnen 72 Stunden erfolgen!

III. Datensicherheit – Data-Breach-Meldung an DSB (Art 33 DSGVO)

- **Mitteilung durch Verantwortlichen an die Behörde**
  - unverzüglich (max. 72 Stunden – Möglichkeit der schrittweisen Meldung, Verzögerung ist mit der Meldung zu begründen)
  - Ausnahme: keine Gefahr für betroffene Personen
- **Inhalt der Meldung**
  - Beschreibung des Vorfalls
  - Angabe der betroffenen Datenarten, der Anzahl der betroffenen Personen, sowie der Zahl der Datensätze
  - Nennung des Ansprechpartners beim Verantwortlichen
  - Abschätzung der Folgen für die Betroffenen
  - Beschreibung der ergriffenen Maßnahmen
- **Aufzeichnungspflicht von Verantwortlichen über Vorfälle**
- **Auftragsverarbeiter müssen Verantwortliche unverzüglich über festgestellte Vorfälle informieren**

III. Datensicherheit – Data-Breach-Benachrichtigung betroffener Personen (Art 34 DSGVO)

- **Mitteilung durch Verantwortliche an Betroffene**
  - Unverzüglich
  - Ausnahme: kein hohes Risiko für persönlichen Rechte und Freiheiten des Betroffenen
- Meldung soll inhaltlich ident mit jener an die Behörde sein!
  - **Ausnahmen**:
    - Die personenbezogenen Daten waren verschlüsselt;
    - Der Verantwortliche kann die hohen Risiken für die Betroffenen durch das Ergreifen von Maßnahmen abwenden;
    - Unverhältnismäßigkeit des zu treibenden Aufwands → Öffentliche Mitteilung ist zu erstatten;
- Pflicht zur Verständigung der Betroffenen kann auch von der Behörde auferlegt werden

IV. Exkurs - Betroffenenrechte

- **Bei telefonischem/mündlichem Begehren**
  - Aktenvermerk mit Name und Kontaktdaten des Betroffenen, Inhalt des Gesprächs und Datum verfassen!
- **Weiterleitung des Begehrens noch am selben Tag**
  - Weiterleitung aller Informationen zum Begehren und zur Person an den Datenschutzbeauftragten!
  - Keine Beantwortung und Erledigung der Begehren durch die Mitarbeiter!
- **Achtung: Anträge sind unverzüglich, spätestens innerhalb eines Monats nach Eingang des Antrags zu beantworten und zu erledigen!**

Exkurs - Auskunftsrecht (Art 15 DSGVO)

- **Weiterer Auskunftsumfang:**
  - **Wenn Daten nicht beim Betroffenen erhoben wurden**:
    - alle verfügbaren Informationen über die Herkunft der Daten
  - **Bei automatisierten Einzelentscheidungen und Profiling:**
    - Angaben zur verwendeten Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung
  - **Bei Drittlandübermittlung**:
    - Unterrichtung über geeignete Garantien im Zusammenhang mit der Übermittlung (z.B. BCR, Standardvertragsklauseln, Angemessenheitsbeschluss der Kommission)
- **Fristen: Ein Monat** (bei komplexen Anfragen max. drei Monate)
- **Kosten**: **kostenlos** (angemessenes Entgelt für weitere Kopie(n))

Standardisierte Prozesse zur Auskunftserteilung verringern Arbeitsaufwand!

IV. Datensicherheit - Technische und organisatorische Maßnahmen (I)

- **Zutrittskontrolle**
  - Schutz vor unbefugtem Zutritt zu Datenverarbeitungsanlagen und manuellen Dateien
  - Gilt auch für Kopier- und Faxgeräte!
  - z.B. Schlüssel, Magnet- oder Chipkarten, Alarmanlagen, absperrbarer Aktenschrank, Versperren des Büros, „Clean Desk“-Policy gilt auch für den Schreibtisch!
- **Zugangskontrolle**
  - Schutz vor unbefugter Systemnutzung
  - z.B. Passwörter, automatische Bildsperre am PC, Verschlüsselung von Datenträgern

Keine Weitergabe von Passwörtern! Sichere Auswahl und Aufbewahrung des Passworts! Niemals Datenträger, Smartphones, Tablets etc. unbeaufsichtigt lassen!

IV. Datensicherheit - Technische und organisatorische Maßnahmen (II)

- **Zugriffskontrolle**
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems
  - zB Zugriffsberechtigungssystem, Protokollierung von Zugriffen, periodische Überprüfung von Berechtigungen, insbesondere von administrativen Benutzerkonten
- **Weitergabekontrolle**
  - Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport
  - zB Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur

Achtung: Bei Versand von E-Mails stets Empfänger und Anhang überprüfen!

IV. Datensicherheit - Technische und organisatorische Maßnahmen (III)

- **Eingabekontrolle**
  - Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind
  - z.B. Protokollierung, Dokumentenmanagement
- **Verfügbarkeitskontrolle**
  - Schutz gegen zufällige oder mutwillige Zerstörung bzw Verlust
  - Rasche Wiederherstellbarkeit
  - zB Backup-Strategie, unterbrechungsfreie Stromversorgung, Virenschutz, Firewall, Meldewege und Notfallpläne, Standardprozesse bei Wechsel/Ausscheiden von Mitarbeitern, Installation von Updates

IV. Datensicherheit - Technische und organisatorische Maßnahmen (IV)

- **Korrekte Entsorgung von Dokumenten und Datenträgern**
  - Dokumente und Datenträger mit personenbezogenen Daten sind fachgerecht zu entsorgen
  - Einhaltung von Löschfristen!
  - zB zertifizierte Aktenvernichtungsgeräte, externe Dienstleister
  - Keine Entsorgung im Papierkorb!

- **Korrekter Umgang mit fremden Wechselmedien**
  - Fremde Wechselmedien (zB USB-Sticks) stellen ein hohes Sicherheitsrisiko für das firmeneigene Netzwerk dar!

V. Phishing

- **Phishing**
  - Versuch, über gefälschte Webseiten oderE-Mails an persönliche Daten zu gelangen.
- **Spear Phishing**
  - Der GEZIELTE Versuch, persönliche Daten von ganz bestimmten Personen und/oder Unternehmen zu erhalte, wobei eine gezielte Vorbereitung über Social Media und Internet erfolgt.
- **Trojaner → Backdoor / Rootkits**
  - Programm, das als nützliche Anwendung getarnt in Erscheinung tritt, welches aber im Hintergrund ohne Wissen des Anwenders eine andere Funktion ausführt

V. Phishing – Tipps für Internetuser (i)

- Achten Sie darauf, dass Sie Webseiten stets über eine SSL/TLS-gesicherte Verbindung aufrufen. Die Internetadresse beginnt in diesem Fall mit https. **Bloße http-Verbindungen sind ein Sicherheitsrisiko**.
- Überprüfen Sie, ob das **SSL-Zertifikat** einer Website aktuell ist und von einer vertrauenswürdigen Zertifizierungsstelle ausgestellt wurde – insbesondere bevor Sie Anmeldedaten eingeben.

- Vermeiden Sie die Nutzung von frei zugänglichen VPNs oder Proxy-Servern.
- Meiden Sie öffentliche WLAN-Spots – beispielsweise im Hotel, am Bahnhof oder in Geschäften.

HTTPS-Webseiten erkennen

V. Phishing – Tipps für Internetuser (ii)

- Halten Sie Ihre Passwörter stets auf dem **aktuellsten Stand**, nutzen Sie für jede Anwendung ein eigenes Passwort und verwenden Sie alte Passwörter nicht noch einmal.
- Sollten Sie nicht umhinkommen, auf öffentliche Netzwerke zuzugreifen, vermeiden Sie Downloads, übermitteln Sie keine Anmeldedaten – beispielsweise für Ihr E-Mail-Postfach oder soziale Netzwerke – und nehmen Sie auf keinen Fall Zahlungen vor.
- **Klicken Sie nicht auf Links in E-Mails von unbekannten Absendern, die Sie möglicherweise auf eine mit Malware bestückte Website locken könnten.**
- **Geben Sie niemals ihre Zugangsdaten (zB von Ihrem Mailkonot) auf einer Webseite ein, wenn Sie per Mail mit einem Link dazu aufgefordert werden. Gehen Sie immer SELBST auf die Ihnen bekannte Seite des Providers oder der Domain!**

Phishing-Quiz

https://phishingquiz.withgoogle.com/

V. Wie erkenne ich Phishing-Mails? (i)

- **Grammatik- und Orthografie-Fehler**
  Am einfachsten zu durchschauen sind E-Mails, die in fehlerhaftem Deutsch geschrieben sind. Meistens wurden sie nicht in Deutsch verfasst, sondern sind mit einem Übersetzungsdienst aus einer anderen Sprache übersetzt worden. Ein weiterer Hinweis auf solche E-Mails sind Zeichensatzfehler, wie etwa kyrillische Buchstaben oder auch fehlende Umlaute.

- **Mails in fremder Sprache**
  Ebenfalls schnell als Phishing zu erkennen sind E-Mails, die auf Englisch oder Französisch verfasst sind. Sollten Sie nicht gerade Kunde einer Bank mit Sitz im Ausland sein, können Sie sicher sein, dass Sie (wenn überhaupt) E-Mails von Ihrer Bank nur auf Deutsch bekommen.

V. Wie erkenne ich Phishing-Mails? (ii)

- **Fehlender Name**
  Ihre Bank und andere Geschäftspartner wie zum Beispiel Online-Zahlungsdienste sprechen Sie in E-Mails grundsätzlich mit Ihrem Namen an und niemals mit "Sehr geehrter Kunde" oder "sehr geehrter Nutzer". Sehr raffinierte Phishing-Täter haben aber oftmals auch Ihren Namen schon herausgefunden und schreiben Sie mit persönlicher Ansprache an, zum Beispiel "sehr geehrte Frau Meier" oder "sehr geehrter Herr Müller". Damit versuchen Kriminelle, der E-Mail eine höhere Glaubwürdigkeit zu verleihen.
- **Dringender Handlungsbedarf**
  Wenn Sie via E-Mail aufgefordert werden, ganz dringend und innerhalb einer bestimmten (kurzen) Frist zu handeln, sollten Sie ebenfalls stutzig werden. Insbesondere, wenn diese Aufforderung mit einer Drohung verbunden ist - beispielsweise, dass sonst Ihre Kreditkarte oder Ihr Online-Zugang gesperrt werden.

V. Wie erkenne ich Phishing-Mails? (iii)

- **Eingabe von Daten**
  Die Aufforderung, persönliche Daten sowie möglicherweise PIN oder TAN einzugeben, ist ein weiterer Hinweis. Banken und Online-Zahlungsdienste werden Sie um so etwas nicht per E-Mail bitten. PIN und TAN werden von Geldinstituten niemals telefonisch oder per E-Mail von Banken abgefragt; dies zählt zu den wesentlichen Sicherheitsregeln.
- **Links oder eingefügte Formulare**
  Banken versenden in der Regel keine E-Mails, sondern Briefe. Falls Sie doch E-Mails von Ihrer Bank erhalten, so wird diese keine Dateianhänge (wie Formulare, über die eine Eingabe gemacht werden muss) versenden. Banken und andere Dienstleister versenden nur in Ausnahmefällen E-Mails mit Links, auf die der Empfänger klicken soll. Dann geht es beispielsweise um neue AGBs, niemals aber um das Einloggen in Ihr Kundenkonto. Besser ist ohnehin immer, die Internetseite selbst aufzurufen, indem Sie diese in das Adressfeld des Browsers eintippen.

V. Wie erkenne ich Phishing-Mails? (iv)

- **Bisher noch nie E-Mails von der Bank erhalten oder kein Kunde**
  Wenn Ihre Bank Ihnen nie E-Mails schickt, eventuell Ihre E-Mailadresse gar nicht kennen kann, oder ein anderer Dienstleister sie kontaktiert, mit dem Sie keine Geschäftsbeziehung haben - löschen Sie die E-Mail.
- **Aufforderung zur Öffnung einer Datei**
  In immer mehr Phishing-E-Mails werden die Empfänger aufgefordert, eine Datei zu öffnen, die entweder als Anhang der E-Mail direkt beigefügt ist oder alternativ über einen Link zum Download bereitsteht. In unerwarteten E-Mails dürfen Sie eine solche Datei keinesfalls herunterladen oder gar öffnen. Denn in der Regel beinhaltet diese Datei ein schädliches Programm wie ein Virus oder ein trojanisches Pferd. Lassen Sie sich auch von angedrohten Konsequenzen wie zum Beispiel einer Kontosperrung, der Einschaltung eines Inkassounternehmens oder anderen erfundenen Gründen niemals dazu verleiten, eine beigefügte Datei zu öffnen! Bei E-Mails mit einem Dateianhang sollten Sie grundsätzlich misstrauisch sein.

V. Wie erkenne ich Phishing-Mails? (v)

- **Mailheader**
  Manche Phishing-Mails sind sehr gut gemacht. Die Absender-E-Mailadresse scheint vertrauenswürdig, der Link im Text auch, das Deutsch ist flüssig? Trotzdem muss diese E-Mail nicht echt sein. Auch Absenderangaben von E-Mails lassen sich fälschen. Wenn Sie - um letzte Zweifel auszuräumen - das prüfen wollen, müssen Sie sich den so genannten Mail-Header anschauen. Dort steht die IP-Adresse des Absenders. Nur diese ist fälschungssicher und gibt Aufschluss über den tatsächlichen Absender.

V. Wie schütze ich mir vor Spear-Phishing? (i)

- **Skeptisch bleiben**
  Am besten können sich Nutzer durch eine gesunde Portion Skepsis vor Spear-Phishing schützen. Wer nicht auf unbekannte Links klickt oder unerwartete Dateianhänge öffnet, kann eigentlich nicht Opfer werden. Das Problem allerdings ist, dass solche Angriffe (im Gegensatz zu üblichen Phishing-Mails) sehr gut gemacht sind. Während man bei der üblichen Spam-Mail schon an der Orthografie und so manch unsinniger Behauptung den dubiosen Charakter erkennt, sind Spear-Phishing-Nachrichten sehr viel besser ausgearbeitet. Sie wirken seriös und echt.
- **Kühlen Kopf bewahren**
  Außerdem arbeiten solche Attacken mit Schwächen von Menschen, in erster Linie mit Neugierde und Angst. Wer denkt, er würde etwas Wichtiges verpassen oder übersehen, läuft eher Gefahr, seine Skepsis abzulegen und auf die Masche hereinzufallen. Deshalb versprechen Spear-Phishing-Nachrichten oftmals Informationen, die die eigene Karriere voranbringen könnten, oder treten so autoritär auf, als hätte man bei Missachtung schwere Konsequenzen zu fürchten.

V. Wie schütze ich mir vor Spear-Phishing? (ii)

- **Sensible Daten schützen**
  Spear-Phishing kann nur funktionieren, wenn der Angreifer genug Informationen über das Opfer findet. Die erste Anlaufstelle dafür sind Social-Media-Accounts. Dort sollte man also nicht zu viel von sich preisgeben, schon gar nicht Informationen, die mit der Arbeit zu tun haben. Über Social Engineering versuchen Betrüger weitere Informationen zu bekommen. Auch hier gilt es Vorsicht zu bewahren: Unbekannten sollte man niemals sensible Daten weitergeben, egal wie vertrauenswürdig der Kontakt erscheint.
- **HTML und Bilddownload meiden**
  Eine weitere Sicherheitsvorkehrung im E-Mail-Verkehr ist es, auf HTML zu verzichten und Bilder nicht automatisch nachladen zu lassen. Auf diese Weise wird verhindert, dass schädliche Programme schon beim Öffnen der Nachricht auf den Rechner des Opfers gelangen können.

V. Wie schütze ich mir vor Spear-Phishing? (iii)

- **Anhänge nicht öffnen**
  Anhänge von unbekannten Absendern sollten ohnehin nicht geöffnet werden. Hier muss man zunächst die Identität des Absenders überprüfen. Auch wenn der Absender seriös wirkt, sollte man nie Anhänge von Absendern öffnen, mit denen man noch nicht zuvor kommuniziert hat. Auch wenn der Absender bekannt zu sein scheint: Öffnen Sie keine Dateianhänge, sie Sie nicht von diesem Absender erwarten. Der Rechner des bekannten Absenders könnte bereits von einem Schadprogramm infiziert sein. Fragen Sie im Zweifel persönlich beim Absender nach.
- **URLs und Links genau prüfen**
  Aufpassen sollte man auch bei den Internetadressen, die sich hinter Links befinden. Man kann sie schon sehen, bevor man auf den Hyperlink klickt. Durch URL-Spoofing versuchen Angreifer, ihre Domain wie eine rechtmäßige Adresse aussehen zu lassen. Mit etwas Aufmerksamkeit kann man diesen Trick schnell enttarnen. Adressen, die gekürzt und damit verschleiert wurden, sollten vorher wieder in die Ausgangsform gebracht oder komplett ignoriert werden.

Vielen Dank für Ihre Aufmerksamkeit

Haben Sie noch Fragen?

RA Dr. Rainer Knyrim
ky@kt.at