„WannaCry“ Teil 2: Existenzbedrohende Strafen dank Datenschutz-Grundverordnung!

Praxistipps zum Thema „Gefahrenquelle E-Mail-Programm“: Phishing-Mails und Internet-Betrug

Am 25. Mai 2018 läuft die Übergangsfrist für die europäische Datenschutz-Grundverordnung (EU-DSGVO) aus und deren extrem strenge Regelungen sind anzuwenden. Damit kommt es **zu massiven Änderungen.** Zwei davon: Die Strafen werden gravierend verschärft und die Meldepflichten an die Datenschutzbehörden fallen weg**.** Die neuen Regelungen gelten für alle Unternehmen, die **Finanz- und Versicherungsbranche werden aber wohl besonders streng behandelt** werden, weil sie **sehr viele sensible Daten** (Finanz, Gesundheit, etc.) der Kunden haben. Große Unternehmen werden sich „einiges“ einfallen lassen müssen, Klein- und Mittelbetriebe sollten zwar auch ihre Prozesse näher beleuchten, könnten aber mit der Befolgung **einiger Praxistipps die größten Gefahrenquellen für „Datenverlust“ beseitigen.**

Genau darum geht es heute in diesem Beitrag. Um weitere Aufgaben, wie etwa Datenschutz-Abwägungen, Datenschutzverantwortliche, Mitarbeiter-Schulung etc. wird es in einem der nächsten Beiträge gehen.

Im vorigen BAV-Newsletter haben wir erste Praxistipps gegeben,

- wie man seinen Computer und die Software auf **aktuellstem Stand** hält, um Hackern (die Lücken in der Software ausnutzen) keine Chance zu geben.
- wie sichere und gut merkbare **Passwörter** aussehen.
- weiters über **Verschlüsselung** (von USB-Sticks, externen Festplatten, Laptops etc.) informiert.
- Auch die möglichen **Schwachstellen Dropbox & Cloudsysteme** waren ein Thema.

Hier zum Nachlesen.

Cybercrime wird komplett unterschätzt! Eine Million Österreicherinnen und Österreicher bereits betroffen!

In einer Pressekonferenz berichtete kürzlich der **Versicherungsverband VVO** von einer **aktuellen Erhebung** des Kuratoriums für Verkehrssicherheit (KFV), der zufolge mindestens eine Million Österreicher bereits durch diverse Formen des Internetbetrugs geschädigt wurden und jährlich Schäden von mehreren Millionen verursacht würden. Zwar nennt das Bundeskriminalamt für 2016 „nur“ 13.000 Anzeigen, aber die **Dunkelziffer sei hier sehr hoch,** so der VVO. Gründe dafür sind, dass sich die Menschen schämen, derart hereingefallen zu sein. Und weil es für Firmen geschäftsschädigend sein kann, wenn bekannt wird, dass sie Opfer von Hackern oder Internetbetrügern geworden sind.

Besonders hoch sei der finanzielle Schaden laut Studie bei **Diebstählen von sensiblen Daten.** Und dieser Problemkreis wird durch die neue Datenschutz-Grundverordnung **dramatisch verschärft,** denn diese sieht bei Verlust von Kundendaten Strafen in Millionenhöhe vor.

„Die größte Schwachstelle ist und bleibt der Mensch selber“, so Dr. Littich vom VVO. Daher beschäftigen wir uns im zweiten Teil des Praxistipps zur Datenschutz-Grundverordnung mit der Gefahrenquelle E-Mail, denn oftmals erlangen Hacker Zugang zu fremden Computern über Dateien, die als Anhänge von E-Mails ins System gelangen, E-Mails daher sind eine echte Gefahrenquelle. Im Beitrag geht es konkret um das **Erkennen von Phishing-Mails**, die **Warnliste des Internet Ombudsmanns**, das Nutzen der Info-Seite „Watchlist Internet“ und Tipps, wie man **gefälschte E-Mail-Absender** bzw. gefälschte Webadressen erkennen kann.

A) Gefahrenquelle E-Mail-Programm: Phishing-Mails und Internet-Betrug

Viele Gefahren entstehen, weil man **zu schnell auf ein E-Mail** und die darin enthaltene Datei klickt. Da gibt es viele Tipps, wir haben uns auf einige konzentriert.

Der Internet-Ombudsmann hat z.B. **9 Tipps gegen Phishing-Mails** zusammengefasst, die wir hier gekürzt wiedergeben:

Unter dem **Fachbegriff „Phishing"** versteht man das „Fischen" nach geheimen Zugangsdaten der Nutzer. Man erhält etwa ein E-Mail mit dem Inhalt, dass das Konto gesperrt werden musste und man für weiteren Zugriff daher bitte Benutzer-Name und Passwort auf der nächsten Seite eingeben solle.

Klickt man dann auf den Link im E-Mail geht eine Internet-Seite auf, die z.B. der Bank-Seite täuschend ähnlich sieht, aber in Wirklichkeit eine Seite der Betrüger ist. Nun kann der Betrüger Ihre Eingabe mitlesen und erhält damit Ihren Benutzernamen und Passwort.

Neben solchen **"klassischen" Phishing-Mails werden auch Millionen-Mails verschickt,** die Schadsoftware mitliefern. Wenn Sie dann auf den mitgeschickten Link, das angehängte Bild („Schauspielerin XY nackt") oder die mitgelieferte „Rechnung" klicken, wird die Schadsoftware aktiviert. Und dadurch der PC gesperrt (Lösegeld-Forderung) oder ein Trojaner installiert (der alle Ihre Eingaben mitliest, Ihr Adressbuch kopiert, Ihren PC übernimmt und zu einem Spam-Versender umwandelt usw.).

Früher konnte man solche Phishing-Mails auf einen Blick an Hand der vielen **Rechtschreibfehler erkennen.** Doch mittlerweile ist das nicht mehr ganz so leicht. Manches Mal wird man sogar persönlich, d.h. mit dem richtigen Namen, angesprochen.

Oftmals scheinen diese **Mails von bekannten Firmen** zu kommen, zumindest soll es so aussehen: eine Rechnung von A1, der Österreichischen Post oder DHL, Verbund oder Kreditkartenfirmen, Mahnungen von bekannten Firmen, Sicherheits-Abfragen von Banken etc. (Wie einfach diese **Absende-Adressen gefälscht werden** können, erfahren Sie im letzten Tipp unten anbei.)

Tipp: Watchlist Internet checken
Sollten Sie ein E-Mail erhalten und Sie sich **nicht sicher sein, ob es echt** ist oder nicht, dann können Sie auf der Info-Seite „Watchlist Internet" hier nachlesen. Dort werden sehr aktuell die momentanen Fallen beschrieben und davor gewarnt.

Ist man danach immer noch unsicher (weil man den konkreten Fall nicht gefunden hat), **dann nimmt man sein Telefon und ruft seinen persönlichen Kontakt bei Bank**, Kreditkartenfirma, Unternehmen an, um zu klären, ob diese „seltsame Mail" vom angegebenen Absender stammt.

Auch der Internet Ombudsmann (von Sozialministerium, VKI and Arbeiterkammer) mahnt zu größter Vorsicht. **Hier seine 9 Tipps gegen Phishing:**

1. Grundregel: Unternehmen fragen Sie niemals per E-Mail nach den höchstpersönlichen Zugangsdaten. *Anmerkung: Stimmt nicht immer, wie genau so ein E-Mail einer bekannten österreichischen Bank traurigerweise gezeigt hat…*

2. Klicken Sie nie auf Links in E-Mails oder sonstigen Nachrichten, in denen dazu aufgefordert wird, Konto- oder Login-Daten oder sonstige nähere Informationen bekannt zu geben.

3. Löschen Sie verdächtige E-Mails sofort!

4. **Öffnen Sie keinesfalls unbekannte Datei-Anhänge** in E-Mails oder sonstigen Nachrichten – darin ist oft Schadsoftware versteckt.

5. Übermitteln Sie keine vertraulichen Daten (Login-Daten, Passwörter, TANs etc.) per E-Mail, via Link oder telefonisch, wenn Sie angerufen werden.

6. Geben Sie vertrauliche und persönliche Daten ausschließlich über **SSL-verschlüsselte** Seiten bekannt (erkennbar an "http**S**://" am Beginn der Internetadresse und an einem **Schlosssymbol** am unteren Bildschirmrand).

7. **Melden Sie** überraschende Änderungen der vertrauten Login-Seiten sofort an den Betreiber (also beispielsweise die Bank oder das Internetportal). Anmerkung: Ebenso dem Internet Obmann bzw. Watchlist Internet. Etwa hier…

8. Geben Sie die **Internetadresse direkt in die Adresszeile** des Internetbrowsers ein, anstatt auf Links zu klicken. *Anmerkung: Links können auf eine ähnliche Adresse umgeleitet werden, ohne dass es Ihnen auffällt.*

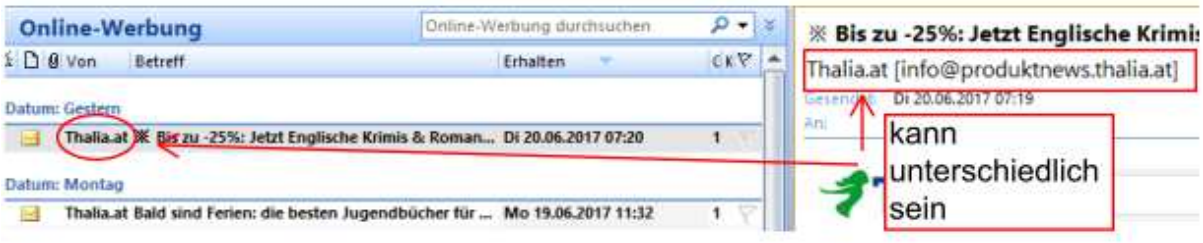
9. Führen Sie laufend, am besten automatisiert, **Sicherheits-Updates** der von Ihnen verwendeten Software durch. *Anmerkung: Siehe obigen Praxistipp b1)*

Ergänzung: Nicht nur bei Mails von Unbekannten sollten Sie misstrauisch sein. Auch wenn Sie Mails von Ihnen bekannten Personen empfangen, sollten Sie nicht komplett gutgläubig sein. Immerhin könnte sein, dass der sendende PC bereits ein Hacker-/Viren-Opfer ist und sich der Virus von selbst und im Namen des Bekannten an Sie weiterverschickt. Also nie gedankenlos auf Mails und deren Anhänge klicken.

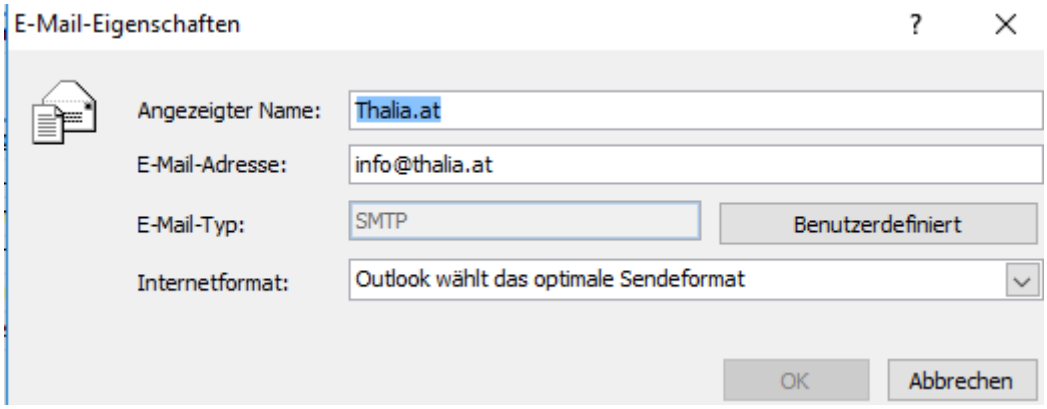
B) Echten E-Mail-Absender bzw. echte Link-Adresse feststellen

Zwischen angezeigtem und tatsächlichem Absender kann es gravierende Unterschiede geben. Das machen sich Spamer und Hacker zu Nutze, um Sie in die Irre zu führen.

Sehen Sie sich die folgende Graphik näher an.
Links sehen Sie unter „VON", dass ein E-Mail von **„Thalia.at**" eingelangt sei.
Rechts sehen Sie, dass sich hinter dem Absender „Thalia" die E-Mail-Adresse info@produktnews.thalia.at versteckt. Das ist die wahre E-Mail-Adresse.



Der vordere Teil der E-Mail-Adresse ist der sogenannte **„Angezeigte Name",** den man beim Installieren eines E-Mail-Kontos beliebig wählen kann. In unserem Beispiel ist das jedes Mal THALIA, passt also zusammen. Bei Betrügern ist das nicht der Fall.

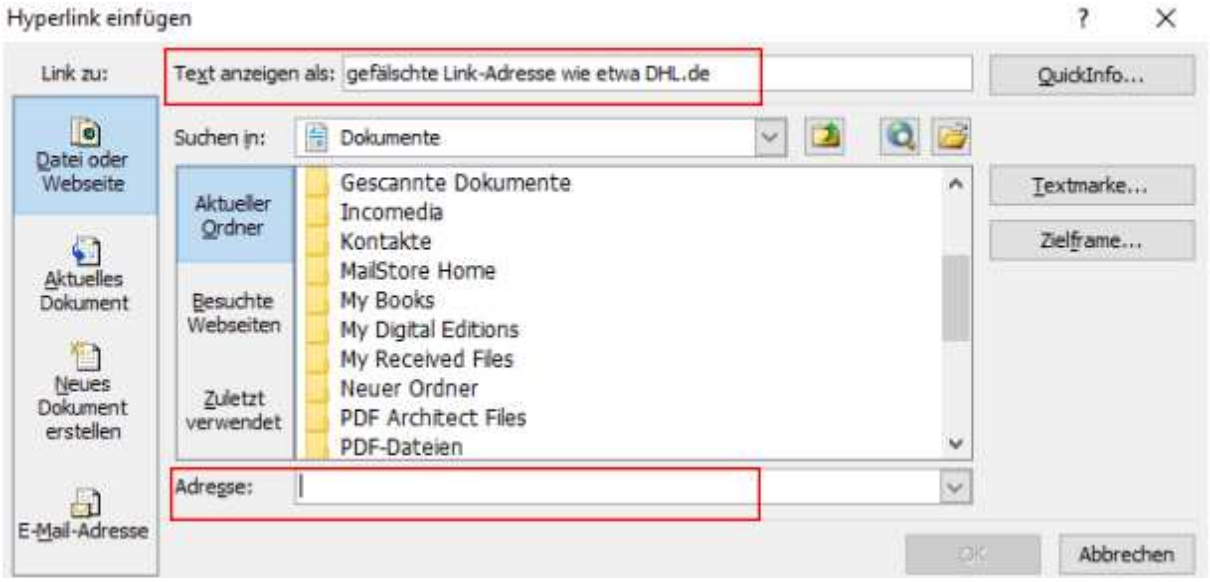


Spam-Absender und Betrüger nutzen diese Möglichkeit aus und tragen einen gefälschten Namen unter „Angezeigter Name" ein. Sagen wir DHL.de, um Sie anzulocken und zu motivieren, das E-Mail und die entsprechenden Anhänge anzuklicken.
Sie müssen also in Ihrem **E-Mail-Programm einstellen,** dass man Ihnen die vollständige E-Mail-Adresse anzeigt.

Dadurch erkennen Sie z.B. dass hinter „DHL.de" in Wirklichkeit z.B. alina17@kiew.ru.com steckt.

Outlook® zeigt grundsätzlich immer nur den Anzeigenamen an, nicht aber dessen E-Mail-Adresse. Man kann sich aber ein kleines Zusatzprogramm installieren, das diesen Mangel von Outlook bereinigt. Hier downloaden.

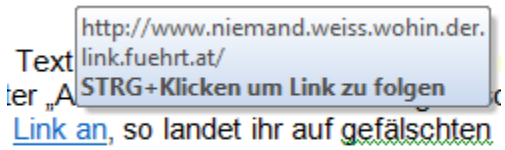
Auch Links im Internet können gefälscht sein, analog zur oben bei E-Mail-Adressen beschriebenen Logik. Schauen Sie sich wieder die **Grafik näher** an:



Wenn man einen Link erstellt, gibt es wiederum ein **Feld „Text anzeigen als"**. Hier kann man jeden beliebigen Text eingeben, also auch www.dhl.de. Darunter aber – im **Feld „Adresse" –** gibt man dann als Fälscher nicht die echte Link-Adresse, sondern eine falsche ein.

Oft wird ganz bewusst ein unbedenklicher Text angezeigt, der manchmal sogar nach der echten Webseite benannt ist. Aber unter „Adresse" wird dann die der gefälschten Webseite eingetragen. Klicken Sie diesen Link an, so landen Sie auf einer gefälschten Webseite.

Tipp: Um die echte Adresse eines Links zu erkennen, gehen Sie **mit der Maus auf den Link, OHNE jedoch zu klicken.** Dann zeigt sich der Link ganz automatisch. Zum Beispiel so:



Wenn der angezeigte Text des Links und die echte Adresse nicht übereinstimmen, dann Hände weg!

Quellen: Mag. Günter Wagner, B2B-Projekte; Mag. Georg Markus Kainz, Quintessenz; Internet Ombudsmann; Watchlist Internet; chip.de; pcwelt.de; Newsletter Tele 2; Outook.com; medianet.at;