# EDV-Sicherheit: Warnbeispiel und Praxistipps

Watchlist Internet warnt topaktuell vor betrügerischen SMS, E-Mails und Anrufen.
Und: Wie kann man echten Absender bei E-Mails oder Links herausfinden?

Nicht nur wegen der **DSGVO** muss man sich mit der EDV-/Datensicherheit beschäftigen, sondern auch deshalb, weil bei Problemen das eigene Geschäft darunter massiv leiden kann, wie das Beispiel Salzburg-Milch zeigen soll.

Seit Monaten kann man von **schweren Hacker-Attacken** mit verbundenen Erpressungsversuchen in den Medien lesen. Es trifft Kleine, aber auch Große. Etwa war Salzburg-Milch tagelang beeinträchtigt, weil die Computersysteme komplett verschlüsselt worden waren, um eine Lösegeld-Zahlung zu fordern. Nachdem das Unternehmen das verweigerte – weil man umfangreiche Back-ups hatte – war der **tägliche Betrieb trotzdem eine Woche massiv eingeschränkt.**

In folgender Reportage berichten wir über Details dieses **„Warnbeispiels", konkret Salzburg-Milch, und bringen dann zwei Praxistipps,** mit denen man weniger oft in Internet-Fallen tappt.

Zurück zum **Desaster von Salzburg-Milch,** nachzulesen im Profil-Bericht vom 15.8.2021. „Nichts ging mehr. Sämtliche Passwörter waren geändert, kein Zugriff auf das IT-System mehr möglich, kein File-Server mehr zugänglich, kein Mail-Server, keine Buchhaltung, keine Verrechnung, keine Logistik, kein Lager." Die Höhe der Forderung sei „erheblich" gewesen, berichtete Salzburg-Milch GF Andreas Gasteiger, werde aber nicht öffentlich genannt. **Glück für Salzburg-Milch war,** dass ein wesentlicher Produktions-Baustein über ein anderes System lief. Und daher konnte man weiterhin Milch von Bauern abholen und verarbeiten. „Dass wir noch einen Fuß in der vordigitalisierten Welt hatten, **hat uns gerettet."**

Die **zunehmende Digitalisierung** spielt also den Hackern und Cyber-Erpressern zunehmend in die Hände. Und diese zunehmende Abhängigkeit schlägt sich auch in **gestiegenen Lösegeld-Forderungen** nieder: Laut IT-Sicherheitsunternehmen Coveware betrug die durchschnittliche Höhe je Forderung im Jahr 2018 noch USD 7.000, 2019 bereits USD 41.000 und 2020 bereits mehr als **USD 200.000.**
Diese Entwicklung sollte auch der Finanz- und Versicherungsbranche eine Warnung sein.

**Salzburg-Milch hatte ein Back-up, das nur 10 Stunden alt war.** Eigentlich ein sensationell guter Wert. Aber was alles in 10 Stunden passieren kann, zeigte sich z.B. im vollautomatisierten Lager, das 100 Meter lang, 25 Meter hoch ist. Und wo nur der Computer weiß, wo sich welche Waren befinden. Alleine in diesen 10 Stunden wurden 1.500 Paletten bewegt. Und mussten nun mühsam händisch recherchiert werden. **In den nächsten 7 Tagen – inklusive Wochenende** – mussten die rund 400 Mitarbeiter aller Abteilungen **an der Wiederherstellung** des Original-Zustandes arbeiten, aber auch viele Arbeiten mit händischen Lieferscheinen etc. durchführen. „Wir haben die Systeme dann Schritt für Schritt neu aufgesetzt, nicht nur die Server, sondern auch sämtliche Arbeitsgeräte und Laptops."

Salzburg-Milch stellte sich natürlich die Frage, **wie es den Hackern gelungen sein könnte, in die Systeme einzudringen.** Ob es darauf eine Antwort gibt, verrät der Profil-Bericht nicht.

Aber immer wieder zeigt sich, dass der **Mensch die größte Schwachstelle ist**. Zu schnell und **unbedacht wird in E-Mails auf Fotos, angehängte Dokumente, Links etc. geklickt.** Und damit lädt man sich Schadsoftware auf den PC und dadurch ermöglicht man den Hackern Zugang sogar zu wirklich gut geschützten Systemen.

**Tipp 1: Watchlist Internet-Webseite und Newsletter**
Um genau für dieses „Problem Mensch" ein ständiges Problembewusstsein zu erzeugen und zu erreichen, dass immer weniger Menschen in Fallen tappen, gibt es das Projekt „Watchlist Internet", das auf aktuelle Betrugsmaschen, Fallen und Fakes im Internet hinweist. Es handelt sich um ein **Projekt des Internet Ombudsmanns** und wird u.a. in Zusammenarbeit mit dem Bundesministerium für Arbeit, Soziales und Konsumentenschutz umgesetzt.

Man informiert, welche Betrugsfälle im Internet aktuell passieren und gibt Tipps, wie man sich vor gängigen Betrugsmaschen schützen kann. Opfer von Internet-Betrug erhalten konkrete Anleitungen für weitere Schritte.

**Wir empfehlen,** sich in die Newsletter-Liste einzutragen — hier klicken – denn dann erhält man jeden Freitag einen kurzen Info-Newsletter, der die aktuellen Gefahren kurz beschreibt und zu weiteren Infos verlinkt.

**Typische Beispiele** der letzten Wochen aus dem Watchlist-Newsletter:

**1. Betrug mit angeblichen Nachrichten des Mobilfunkbetreibers**
Erneut werden massenhaft betrügerische SMS ausgeschickt. Es soll sich um eine „Neue Nachricht des Mobilfunkbetreibers" handeln. Für mehr Infos soll man einem Link folgen. Achtung: Der Link führt auf eine betrügerische Website mit Schadsoftware! Die Nachricht kommt nicht vom Netzbetreiber.
Link zu den News: <http://www.watchlist-internet.at/index.php?RDCT=4126e8b4e852866584ce>

**2. Vorsicht vor Microsoft-Anrufen**
Legen Sie sofort auf, wenn Sie angeblich von Microsoft angerufen werden. Kriminelle geben sich als Microsoft-MitarbeiterInnen aus und behaupten, sie hätten auf Ihrem Computer einen Virus entdeckt. Die Fake-Microsoft-MitarbeiterInnen verwickeln Sie dann in ein Gespräch und bieten Ihnen an, das Problem gemeinsam zu lösen. Achtung: Es handelt sich um eine Betrugsmasche!
Link zu den News: <http://www.watchlist-internet.at/index.php?RDCT=57888bd39cd276cdb891>

**3. SMS: Vorsicht vor gefälschter Sendungsverfolgung**
Kriminelle versenden momentan per SMS gefälschte Paketinformationen zu einer Bestellung. In der Nachricht heißt es, dass Ihr Paket nicht zugestellt werden konnte oder eine Sendungsverfolgung nun möglich ist. Sie werden aufgefordert, auf einen Link zu klicken. Achtung: Der Link führt in eine Internetfalle.
Link zu den News: <http://www.watchlist-internet.at/index.php?RDCT=33f0a12a790e050114e8>

Zusätzlich kann jede und jeder über ein Meldeformular **selbst Internet-Fallen melden:** Das Formular finden Sie hier … oder senden Sie ein E—Mail an: meldung@watchlist-Internet.at

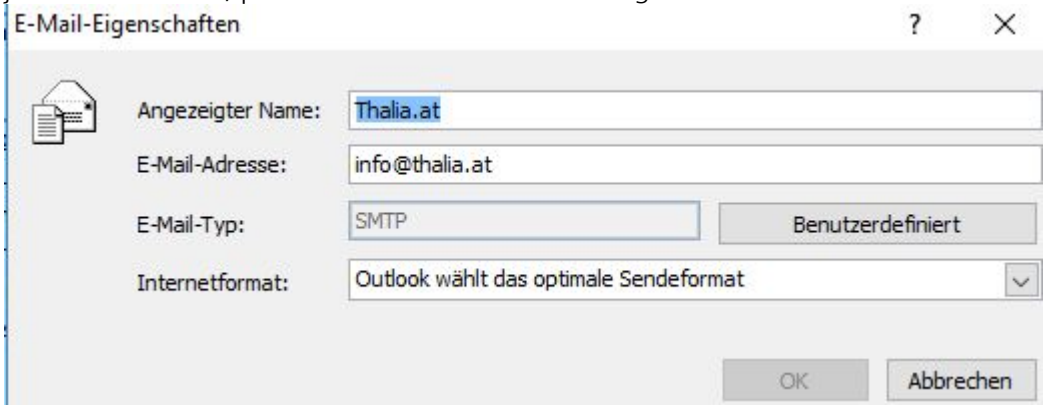
**Sollten Sie bereits Opfer von Online-Betrug geworden sein,** können Sie sich an den Internet Ombudsmann (mehr dazu unter https://ombudsmann.at) und mit einer Betrugsanzeige direkt an die Polizei wenden.

**Tipp 2: Echten E-Mail-Absender bzw. echte Link-Adresse feststellen**
Zwischen angezeigtem und tatsächlichem Absender kann es gravierende Unterschiede geben. Das machen sich Spammer und Hacker zunutze, um Sie in die Irre zu führen.

**Sehen Sie sich die folgende Grafik 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. Bei Internet-Betrugs-Versuchen steht **hinten meist GANZ WAS ANDERES.**


Das **Problem liegt in einem Struktur-Mangel von Mail-Programmen.** Dort kann man nämlich beliebige Texte eintragen.

Der vordere Teil der oben gezeigten E-Mail-Adresse (hier also „Thalia.at") 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.



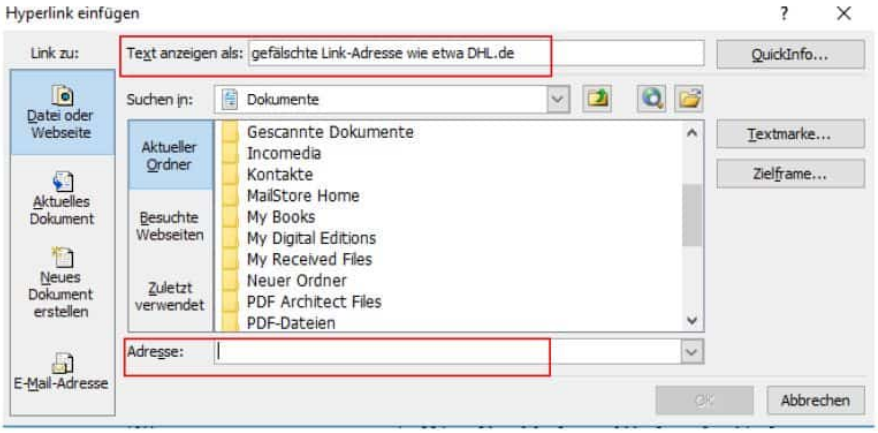

**Spam-Absender und Betrüger nutzen diese Möglichkeit aus** und tragen einen gefälschten Namen unter „Angezeigter Name" ein. Sagen wir BAWAG P.S.K., um Sie anzulocken und zu motivieren, das E-Mail und die entsprechenden Anhänge anzuklicken. Tatsächlich ist es aber ein Spammer, ein Hacker etc. der Sie in die Irre führen möchte.

**TIPP:** Sie müssen also in Ihrem **E-Mail-Programm einstellen,** dass man Ihnen die **vollständige E-Mail-Adresse anzeigt.**

Und dann schaut die Mail-Anzeige PLÖTZLICH SO AUS:


Aus dem vertrauenswürdigen Absender BAWAG wird plötzlich eine obskure **E-Mail-Adresse!**

**ACHTUNG: 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"** und 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 Adresse der gefälschten Webseite eingetragen. Klicken Sie diesen Link an, so landen Sie auf der gefälschten Webseite.

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


**Wie oben beim Thema E-Mail-Adresse festgestellt, gilt auch hier: Wenn der angezeigte Text des Links und die echte Adresse nicht übereinstimmen, dann Hände weg!**

Quellen: Mag. Günter Wagner, B2B-Projekte für Versicherungsbranche, Homepage Watchlist Internet und Internet-Ombudsmann, Profil-Beitrag „Salzburg Milch you are fucked" vom 15.8.21