Datenschutz News 2019 – 06

datenschutz-link.de
SABINE LINK
DATENSCHUTZBEAUFTRAGTE

Herzlich willkommen bei meinen Datenschutz-News, Ausgabe Dezember 2019

Zum Jahres-Endspurt nochmals einige Datenschutz-Informationen, verbunden mit den besten Wünschen für eine erfolgreiche und schöne Adventszeit, frei von bösen Überraschungen.

Adventskalender zur IT-Sicherheit

Geschenke sind schön! Bei https://www.sicher-im-advent.de/ finden Sie einen Adventskalender mit nützlichen Informationen zur IT-Sicherheit. Jeden Tag ein Türchen zu öffnen und so die Aufmerksamkeit auf IT-Sicherheit zu richten, das ist eine pfiffige Idee, auf die ich gerne hinweisen möchte.

*****

Adventskalender zur IT-Sicherheit

Fake-Shops, Mail-Abzocke und Windows 7-Supportende

Das krasse Gegenteil von guten Taten sind kriminelle Aktionen, die unsere Weihnachtsstimmung ausnutzen wollen. Bei Kriminellen ist es leider beliebt, das „Trusted-Shops“-Symbol auf ihre Fake-Shop-Internetseite zu setzen, um Seriösität vorzugaukeln. Ein echtes „TrustedShops“-Gütesiegel ist klickbar und verlinkt auf die Seite https://www.trustedshops.de, wo das zu diesem Shop gehörige Gütesiegel-Zertifikat angezeigt und dessen Gültigkeit bestätigt wird.

Fake-Shops

„trustedshops“-Siegel ist entweder anklickbar oder gefälscht

E-Mails mit Schad-Anhang tauchen in immer neuen Variationen auf. Sensibilisieren Sie Ihre Mitarbeiter regelmäßig! Gerade „Bewerbung / Rechnung / Ihre Bestellung / Ihr Konto / Protokoll / Vertrag / eilig“ sind als Betreff krimineller Mails beliebt, weil solche E-Mails im Büroalltag oft vorkommen. Ein routiniertes schnelles Anklicken kann dann direkt ins Verderben führen. Zwei „Design-Typen“ von kriminellen E-Mails treten derzeit gehäuft auf, davor möchte ich warnen:

Zwei typische Designs von kriminellen Mails

In einem gut gemachten Anschreiben werden ein seriöser Inhalt und eine wichtige vertrauliche Information vorgegaukelt, es ist ein verschlüsselter Anhang beigefügt und das Passwort zum Öffnen des verschlüsselten Anhangs ist gleich in der Mail genannt, als zuvorkommender Service des Cyberkriminellen. Dieser Trick nutzt es aus, dass die Firewall- und Antiviren-Programme, die in der Lage sind, virenverseuchte E-Mailanhänge zu erkennen und abzufangen, bei einem verschlüsselten Anhang oft nicht funktionieren. Damit die Falle zuschnappt, muss der verschlüsselte Anhang geöffnet werden, daher wird dem arglosen Empfänger das Passwort gleich mitgeteilt.

Verschlüsselter Anhang einer gut formulierten „vertraulichen Mail“

Fazit: Wenn bei einer verschlüsselten Mail das Passwort gleich mitgeliefert wird, diese Mail sofort löschen, nichts anklicken, nichts öffnen! Wer in seriöser Absicht eine verschlüsselte Mail schickt, wird das Passwort immer mit einem anderen Medium (SMS, Telefon, Post) mitteilen, niemals in derselben Mail.

das Passwort ist gleich dabei… nie öffnen!

RA Sabine Link – Datenschutzbeauftragte • Schulte-Marxloh-Str. 19 • 47169 Duisburg • info@datenschutz-link.de
Telefon 0176-8488 5082 oder 0203-3498 3045 • USt-Id DE298 214 620 • Nationalbank • DE20 3602 0030 0000 2490 68

Der andere Crime-Design-Typ täuscht einen Absender aus derselben Firma vor. Mails an Name@firma.de scheinen von vorstand@firma.de zu kommen, IT@firma.de oder einem anderen Phantasie-Absender, an „Liebe Kolleg*innen“, verbunden mit einem „interessanten“ oder „wichtigen“ Hyperlink zum Anklicken, z.B. für ein „Sicherheits-update“ aller IT-Nutzer oder einem Anhang, der „Scan2462345-2019“ oder ähnlich heißt, als stamme dieser Anhang aus dem hauseigenen Scanner. Fazit: Auch bei vermeintlich bekannten Mail-Absendern immer misstrauisch bleiben, **vor jedem Anklicken erst nachdenken**!

IT-Sicherheit ist ein ständiger Wettlauf. Da die Kriminellen alle IT-Innovationen schnell nutzen, zwingt uns die Dynamik der IT-Entwicklung zu ständigen Aktionen und Investitionen für IT-Sicherheit. Software muss ständig durch Sicherheits-Updates gepflegt werden.

Wer noch Windows 7 einsetzt, ist davon aktuell betroffen: Der Support wird Ende Januar 2020 eingestellt, also schnell umstellen auf Windows 10, fragen Sie Ihre IT-Ansprechpartner!

Auch 2020 wird wieder spannend.

Mailabsender aus der eigenen Firma, von „Vorstand“, „IT“, etc. , mit einem Hyperlink zum Anklicken: Eilig, zur Sicherheit, für ein System-Update… VORSICHT!

Kollegen / Vorgesetzte ansprechen und nachfragen

Dynamik ohne Pause, permanente Sicherheitsupdates, Supportende bei Windows7

*** *** *** *** *** *** *** ***

Bei allen meinen Kunden und Geschäftspartnern bedanke ich mich sehr herzlich für die gute Zusammenarbeit in diesem Jahr!

Ich wünsche Ihnen/Euch
Fröhliche Weihnachten, gemütliche Festtage
und für das Neue Jahr 2020
alles Gute!

Impressum: RA Sabine Link
Datenschutzbeauftragte und Unternehmensberatung
Schulte-Marxloh-Str. 19, 47169 Duisburg
Telefon: 0176-8488 5082 oder 0203-3498 3045
Internet: www.datenschutz-link.de
E-Mail: info@datenschutz-link.de
Umsatzsteueridentifikationsnummer: DE 298 214 620
Verantwortlich für den Inhalt: RA Sabine Link, Anschrift siehe oben.

Plattform der EU-Kommission zur Online-Streitbeilegung: www.ec.europa.eu/consumers/odr .

Die Berufshaftpflichtversicherung (Vermögensschaden-Haftpflichtversicherung) besteht bei der ERGO Versicherung AG, Victoriaplatz 1, 40477 Düsseldorf. Räumlicher Geltungsbereich: Europa.

Die gesetzliche Berufsbezeichnung „Rechtsanwalt“ wurde in der Bundesrepublik Deutschland verliehen. RA Sabine Link ist Mitglied der Rechtsanwaltskammer Düsseldorf.

Anschrift der zuständigen Rechtsanwaltskammer:
Rechtsanwaltskammer Düsseldorf
Freiligrathstraße 25, 40479 Düsseldorf
http://www.rechtsanwaltskammer-duesseldorf.de.
Für Rechtsanwälte gelten die folgenden berufsrechtlichen Regelungen: Bundesrechtsanwaltsordnung BRAO, Berufsordnung für Rechtsanwälte BORA, Fachanwaltsordnung FAO, Rechtsanwaltsvergütungsgesetz RVG. Diese Regelungen finden Sie auf www.brak.de/fuer-anwaelte/berufsrecht/