UIMCommunic@tion

01/2021

Ausgabe für Deutschland

*Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert*

# HTTPS-Links und Emotet erhöhen die Gefahren bei Phishing-Attacken

## Sicherheitsstrategie und Sensibilisierung der Mitarbeiter helfen gegen Angriffe

*Das Fischen nach Passwörtern hört sich harmloser an, als es in der Realität ist. Denn Phishing steht am Anfang unterschiedlicher Delikte, die vom „einfachen" Datendiebstahl über illegale Kontoabbuchungen bis hin zu Erpressungen von Lösegeld reichen. „Dabei sind die Opfer sowohl große oder sogar größte Unternehmen als auch Einzelpersonen", weist der langjährige Informationssicherheitsexperte Dr. Jörn Voßbein auf die sehr heterogene Gruppe von Betroffenen hin. Außerdem zeigt der Lagebericht des Bundesamtes für Sicherheit in der Informationstechnologie (BSI), dass die Täter sehr flexibel auf gesellschaftliche Entwicklungen reagieren. Phishing ist, das zeigt der BSI-Lagebericht, in den letzten Monaten durch den vermehrten Einsatz von HTTPS-Links noch bedrohlicher geworden. Was das bedeutet und wie man sich schützt, lesen Sie im Weiteren.*

Neben Phishing kommen ebenfalls Schadprogramme für die illegale Datenaneignung und den folgenden Missbrauch von Identitätsdaten zum Einsatz. Das Schadprogramm Emotet bildet die Grundlage für die Erbeutung von Daten und die nachfolgenden Angriffe. Emotet liest die Kontaktbeziehungen und E-Mail-Inhalte aus den Postfächern infizierter Systeme aus. Diese Informationen verwenden die Angreifer im Anschluss daran zur weiteren Verbreitung des Schadprogramms. Der große Erfolg von Emotet beruht darauf, dass die E-Mails besonders authentisch wirken und so die Opfer erfolgreich zum Öffnen verleiten.

Der Einsatz von HTTPS-Links entwickelt sich in Phishing-Mails immer mehr zum Standard. Dies wohl auch deshalb, weil Links auf HTTP-Basis inzwischen von gängigen Browsern negativ gekennzeichnet werden. Hypertext Transfer Protocol Secure (HTTPS) steht für eine verschlüsselte sowie gegen Manipulation geschützte Datenübertragung und verstärkt insofern den Eindruck von Vertrauenswürdigkeit und Seriosität von Internetseiten, auch wenn es sich in dem Falle um Phishing-Seiten handelt. Mehr als jede zweite Phishing-Mail (60 Prozent) verwendete mittlerweile laut Verbraucherzentrale NRW einen Link auf HTTPS-Basis. Allerdings spielt die HTTPS-Basis nur Seriosität vor, denn die dafür notwendigen Zertifikate können kostenfrei im Internet bezogen werden. Sicherheitsforscher entdeckten Ende 2019 mehrere ungesicherte Datenbanken eines Technologieunternehmens mit Kunden- und Supportinformationen. Die große Menge von veröffentlichten privaten Krankenakten lässt ebenfalls alle Alarmglocken schrillen. Schließlich handelt es sich um hochsensible personenbezogene Daten, die in der Öffentlichkeit nichts zu suchen haben, für die Betroffenen schweren Schaden anrichten können und aus diesen Gründen einen besonders hohen Schutzbedarf haben.

„Die Vielfalt und Häufigkeit von Vorfällen, bei denen immer wieder sensible Daten unfreiwillig veröffentlicht werden, sind alarmierend", erklärt Informationssicherheits-Fachmann Dr. Jörn Voßbein. Er und die Experten von UIMC raten zu einer nachhaltigen Informationssicherheits-Strategie. Diese beinhaltet sowohl eine technische Überprüfung der bisher eingesetzten Programme verbunden mit einem wiederkehrenden Update in Bezug auf Sicherheit. „Die Schulung und Sensibilisierung der eigenen Belegschaft für das Thema Daten- und Informationssicherheit ist die zweite Säule einer erfolgreichen IT-Sicherheitsstrategie und darf nicht unterschätzt werden, schließlich bedürfen die meisten Phishing-Attacken noch eine Aktion eines überrumpelten Mitarbeiters", erläutert Dr. Voßbein. Alles mit dem Ziel, das Fischen nach Daten möglichst erfolglos zu machen und den Cyberkriminellen ihre Geschäfte zu vermiesen.

**Noch Fragen?**
Treten Sie mit uns in einen Dialog ein!

# UIMCommunic@tion

*Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert*

## Brexit-Update

Seit Ende Januar 2020 ist das Vereinigte Königreich, d. h. Großbritannien und Nordirland, kein EU-Mitglied mehr. Zwischen der Europäischen Union und dem Vereinigten Königreich war eine Übergangsvereinbarung getroffen worden.

Im aktuellen Entwurf des Brexit-Abkommens (Stand: 31.12.2020) ist eine **viermonatige Übergangsfrist** ab dem 1. Januar 2021 enthalten. So ist eine Übergangsregelung für Datenübermittlungen vorgesehen, die den befürchteten gravierenden Rechtsunsicherheiten vorbeugt (Article 10A Interim provision for transmission of personal data to the United Kingdom).

Damit sind Übermittlungen in das Vereinigte Königreich vorerst weiterhin unter den bisherigen Voraussetzungen möglich. Gravierende Erschwernisse für die betroffenen Unternehmen werden so zunächst vermieden. Allerdings ist jetzt die EU-Kommission in der Pflicht, tragfähige Adäquanzentscheidungen vorzulegen, die auch die aktuelle Rechtsprechung des Europäischen Gerichtshofs berücksichtigen und von den Mitgliedstaaten genauso wie vom Europäischen Datenschutzausschuss sorgfältig zu prüfen sein werden.

**Empfehlung:** Wir empfehlen, den Prozess weiterhin zu beobachten und sich ggf. auf einen „Nicht-Angemessenheitsbeschluss“ vorzubereiten.

Mehr unter **www.uimc.de/news**

## Reform sichert Zusammenarbeit von EU- & schweizerischen Unternehmen

Das Schweizer Parlament hat beschlossen, das geltende Datenschutzgesetz zu überarbeiten und es so dem Niveau der Europäischen Union anzupassen. Damit gilt die Schweiz auch weiterhin als sicheres Drittland – mit der Folge, dass EU und schweizerische Unternehmen auch künftig ohne größere Hürden zusammenarbeiten können. Die Schweiz ist kein Mitglied der EU, in dem deutschen Nachbarland gilt deshalb nicht die Datenschutzgrundverordnung (DSGVO). Weil das dortige Datenschutzrecht nicht genauso streng ist wie das EU-weite, drohte der Schweiz, den Angemessenheitsbeschluss der EU zu verlieren – und damit den Status als sicheres Drittland.

Mehr unter **www.uimc.de/news**

## [neu] webeCollege

kompakt praxisnah informieren

**Die nächsten Termine [kostenfrei]**

10.03.2021: Die 3 R der DSGVO: Rechenschaft, Risikobewertung und Revision
14.04.2021: 5 Anforderungen, die beim Drittlandtransfer zu beachten sind
15.05.2021: 5 Tipps für rechtskonformes Outsourcing

Mehr unter **www.uimc.de/webecollege**

## Updates/Neue Unterlagen im Online-Formular-Center

In unserem Online-Formular-Center finden Sie viele hilfreiche Muster-Formulare.

Derzeit sind alle Formulare aktuell.

www.online-formular-center.eu

Bitte senden Sie mir neben den angekreuzten Themen weitere Informationen zu:

- ☐ HTTPS-Links und Emotet erhöhen die Gefahren bei Phishing-Attacken
- ☐ Reform sichert Zusammenarbeit von deutschen und schweizerischen Unternehmen
- ☐ **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu!

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 946 7726 9200 oder formlos per Mail an communication@uimc.de

**Mehr Informationen, Hinweise und Tipps finden Sie hier: https://communication.UIMC.de**