TLP: green

Baden-Württemberg
CYBERSICHERHEITSAGENTUR

ERLÄUTERUNG DER SICHERHEITSMASSNAHMEN BEIM E-MAIL-VERSAND

3. März 2022

Erhöhte Sicherheitsmaßnahmen aufgrund des Ukrainekriegs

Derzeit wird die Gefahr gezielter Angriffe auf einzelne Personen sowie das Auftreten von SPAM-Wellen als besonders hoch eingeschätzt. Durch mögliche Kollateralschäden des Cyberkriegs in der Ukraine muss auch mit dem Abfluss von Kommunikation (externer Partner) gerechnet werden, die wiederum für gezieltes Phishing genutzt werden können. Aus diesem Grund hat die BITBW vorübergehend verstärkte Sicherheitsmaßnahmen umgesetzt, die leider auch zu Einschränkungen bei der E-Mail-Kommunikation führen.

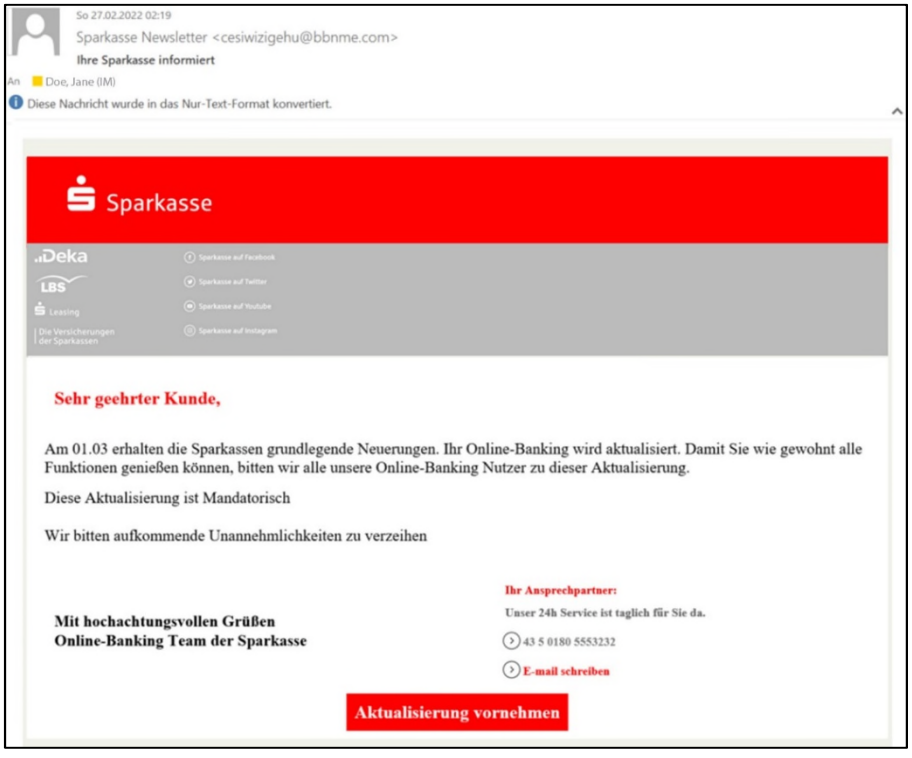
Wieso werden Bilder und Formatierungen in E-Mails gesperrt?

Seit Kurzem werden E-Mails nicht mehr im HTML-Format, sondern nur noch in Textform empfangen. Bilder und Formatierungen werden nicht mehr dargestellt.

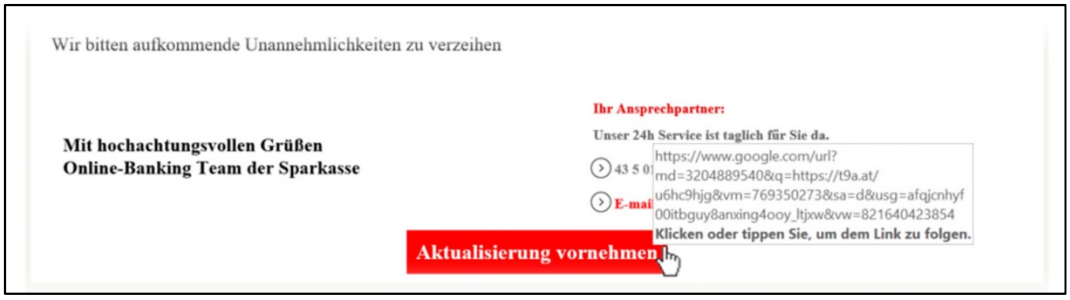
Gefährliche Links hinter scheinbar vertrauenswürdigen Inhalten

Bei E-Mails im HTML-Format, wie sie bisher möglich waren, können Links auf nicht vertrauenswürdige Webseiten verschleiert werden. Wie in der Beispiel-Mail unten zu sehen ist, scheint es sich um eine offizielle Mail der Sparkasse zu handeln. Dahinter verbirgt sich allerdings eine Spam-Mail mit Links auf gefährliche Inhalte.

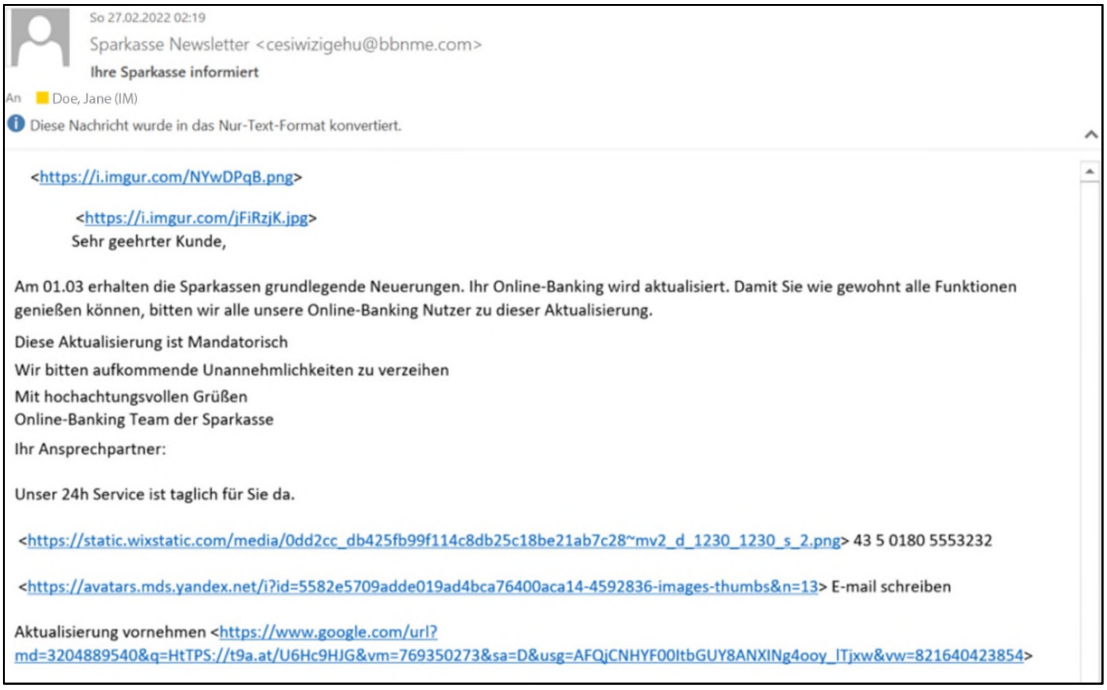
Das ist eine typische Vorgehensweise, um die Empfänger dazu zu bringen, gefährliche Inhalte wie zum Beispiel Trojaner oder Viren auf ihren Computer zu laden. Ein vorschneller Klick kann schon ausreichen, um einen Computer zu infizieren.



Das eigentliche Ziel der Links wird angezeigt, wenn Sie mit der Maus länger auf dem Link bleiben, ohne darauf zu klicken.



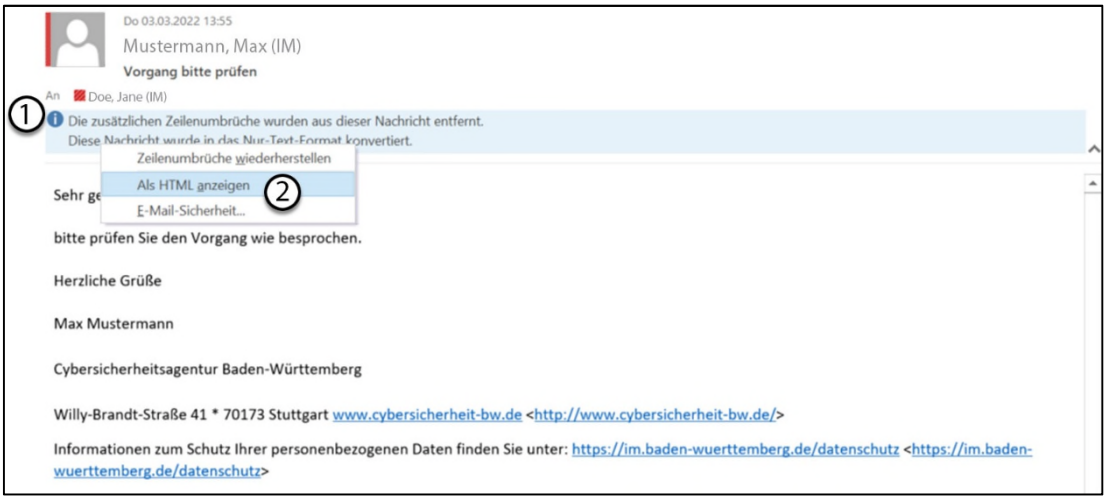
E-Mails im Textformat helfen Ihnen, Spam-Mails zu erkennen
Durch die Deaktivierung des HTML-Formats, wird in den E-Mails nur noch der Text angezeigt. Bei der Beispiel-Mail im Textformat sind die zuvor verschleierten Links nun deutlich als verdächtig zu erkennen.



HTML-Format wieder aktivieren

Wenn Sie den Inhalten einer E-Mail vertrauen, können Sie das ursprüngliche HTML-Format wieder aktivieren. Dadurch werden die Formatierungen und Bilder wieder angezeigt.

Klicken Sie in der Mail auf das **i-Symbol (1)** und anschließend auf **Als HTML anzeigen (2)**.



Die E-Mail wird im ursprünglichen HTML-Format angezeigt.


Do 03.03.2022 13:55
Mustermann, Max (IM)
Vorgang bitte prüfen
An Doe, Jane (IM)

Sehr geehrte Frau Doe,
bitte prüfen Sie den Vorgang wie besprochen.

Herzliche Grüße
Max Mustermann

Baden-Württemberg
CYBERSICHERHEITSAGENTUR
Cybersicherheitsagentur Baden-Württemberg
Willy-Brandt-Straße 41 * 70173 Stuttgart
www.cybersicherheit-bw.de
Informationen zum Schutz Ihrer personenbezogenen Daten finden Sie unter: https://im.baden-wuerttemberg.de/datenschutz

Wieso landen verschlüsselte Dateiarchive (ZIP) in Quarantäne?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat von einem deutlichen Anstieg von E-Mails mit Schadsoftware berichtet. Diese können sich in verschlüsselten ZIP-Archiven befinden. Verschlüsselte Archive können vom Virenscanner nicht geöffnet und somit auch nicht geprüft werden.

Daher werden E-Mail-Anhänge mit **verschlüsselten** Dateiarchiven (z. B. ZIP-Dateien) von externen Absendern in eine Quarantäne verschoben. Bisher wurde so auch mit Office-Dokumenten verfahren, die Makros enthalten. Berechtigte E-Mails können auf Anfrage bei Service-Desk@bitbw.bwl.de freigegeben werden.

Sicherheitsmaßnahmen werden wöchentlich geprüft

Es wird wöchentlich geprüft, ob diese erhöhten Sicherheitsmaßnahmen weiterhin notwendig sind. Sobald sie wieder zurückgenommen werden, werden Sie schnellstmöglich darüber informiert.

Erklärungen zum „Traffic Light Protocol“ (TLP)[1]

TLP:WHITE – Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen dieser Stufe ohne Einschränkungen frei weitergegeben werden.

TLP:GREEN – Organisationsübergreifende Weitergabe

Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.

TLP:AMBER – Eingeschränkte interne und organisationsübergreifende Weitergabe

Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis **Kenntnis nur, wenn nötig** weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen.

Hierfür muss er sicherstellen, dass die Dritten das TLP kennen und die damit verbundenen Regeln einhalten. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen, diese müssen eingehalten werden.

TLP:RED – Persönlich, nur für bekannte Empfänger

Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/ Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt.

Eine Weitergabe ist untersagt. Meistens werden Informationen dieser Stufe mündlich oder persönlich übergeben.

[1] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/KRITIS/Merkblatt_TLP.html, aufgerufen am 8.03.2022, 12:03 Uhr