Wichtige Info: Das CERT BWL warnt!

Die weltweit aktive neue Welle der Schadsoftware EMOTET erreicht aktuell auch unsere Systeme landesweit. Dazu geben das CERT BWL und der Landes-CISO folgende Hinweise mit der Bitte um Verteilung **und dringliche Beachtung**:

EMOTET zeichnet sich dadurch aus, dass mit gefälschten E-Mail-Absender-Adressen und „gestohlenen" echten Betreff-Zeilen **eine Kommunikation mit scheinbar bekannten Absendern vorgetäuscht werden soll.** So sollen die Empfänger zum Anklicken angefügter Dateianhänge verleitet werden.

Neben Anhängen mit der Dateiendung „.doc" **werden neuerdings auch Anhänge mit der Dateiendung „.zip" dazu verwendet.** Besonders heimtückisch dabei ist, dass die .zip-Dateien zusätzlich passwortgeschützt sind, wobei das zum Öffnen der Dateien benötigte Passwort allerdings gleich in der betreffenden E-Mail in Klartext enthalten ist. Durch diesen Passwortschutz können die Virenscanner die Datei nicht öffnen und untersuchen!

Daher: Wo die Technik an ihre Grenzen stößt, ist umso mehr unsere eigene Umsicht gefragt. Helfen Sie mit!

Wie können Sie zum Schutz unserer Systeme und Ihrer Daten in der Landesverwaltung beitragen?

Die wichtigste Maßnahme ist, bei jeder E-Mail, die Sie zum Öffnen eines Anhangs oder zum Anklicken eines Links auffordert, Vorsicht walten zu lassen.

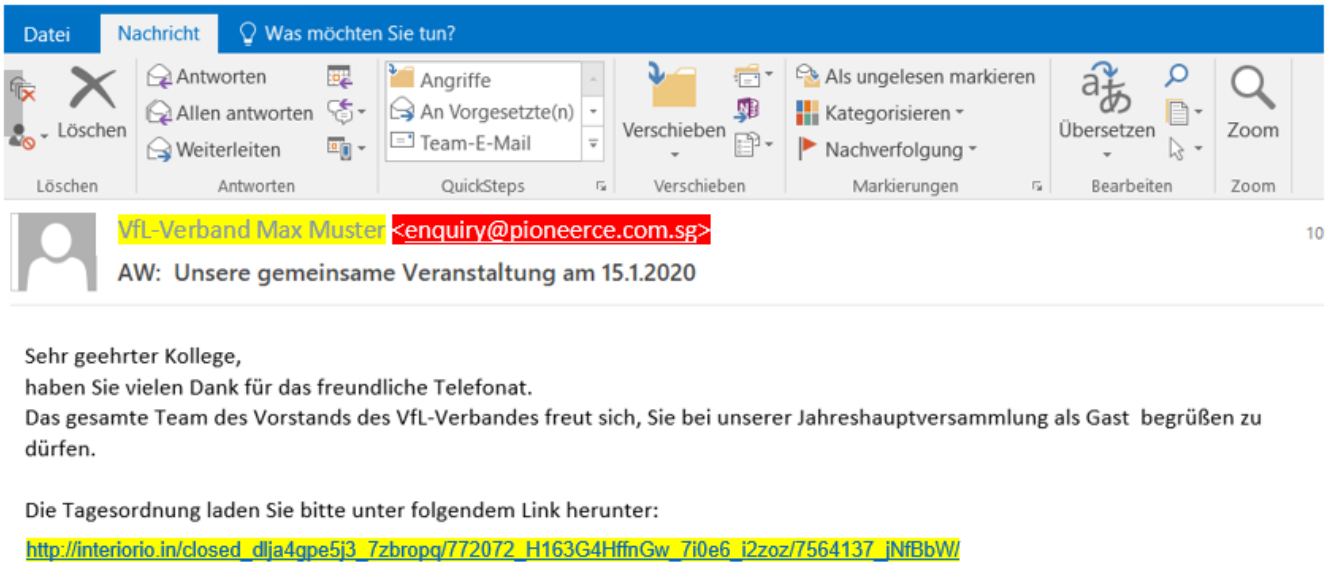
Schauen Sie sich den Absender und die Absende-Adresse ganz genau an. Vermeiden Sie es unbedingt, Anlagen von Absendern zu öffnen und Links in E-Mails anzuklicken, deren Identität nicht zweifelsfrei feststeht. Kontaktieren Sie im Zweifel den Absender und fragen sicherheitshalber nach.

Anhand des nachfolgenden Beispiels wollen wir dies nochmals erläutern. Die farbigen Markierungen weißen Sie dabei auf die jeweils relevanten Merkmale in der abgebildeten Beispiel-E-Mail hin.

➔ **Gleichen Sie Absender-Name und E-Mail-Adresse des Absenders ab** : Eingehende Mails zeigen sowohl einen Namen als auch eine <E-Mail-Adresse> an. Der Name ist nahezu beliebig fälschbar, die E-Mail-Adresse dagegen nur schwer. Im angehängten Beispiel sieht man, dass <E-Mail-Adresse> **nicht zum Namen passt**.

➔ **Vermeiden Sie, Links anzuklicken. Achten Sie auf das Aussehen von Links**. Siehe Beispiel: Beginnt ein Link mit „http“ anstelle von „https“, verweist die Endung auf ein fremdes Land (im Beispiel: „.in“ steht für Indien) oder sieht er kryptisch aus, so kann dies ein Indiz für Schadsoftware sein.

➔ **Ist eine E-Mail im Betreff bereits mit „SPAM-Verdacht“ gekennzeichnet,** ist besondere Vorsicht geboten. Mit großer Wahrscheinlichkeit verbirgt sich ein Virus in der E-Mail.



Gerne unterstützt das CERT BWL bei der Beurteilung solcher E-Mails. Wenden Sie sich bei entsprechenden Fragen an cert@bitbw.bwl.de oder fragen Sie Ihre jeweiligen Informationssicherheitsbeauftragten (CISO).

Mit freundlichen Grüßen

Ihr CERT BWL Team
in Kooperation mit dem Landes-CISO