ALTHAMMER & KILL

Mitarbeiterinformation: aktuelle Sicherheitshinweise

Liebe Mitarbeitende,

die aktuelle Situation führt zu einem erheblichen Anstieg zielgerichteter Angriffe auf Einrichtungen des Gesundheitssektors. Täter nutzen dabei Ihre Aufmerksamkeit auf wichtigere Dinge aus. Sie verleiten den Nutzer zum Klick auf gefährliche Links, Preisgabe von sensiblen Informationen, falsche Überweisungen oder Bestellungen auf Fake-Shops. Hinzu kommt derzeit oft, dass sich die IT wegen zusätzlicher Aufgaben durch Home-Office, Videokonferenzen oder auch Krankheit weniger um mögliche Abwehrmaßnahmen kümmern kann. Auch der Einsatz privater Geräte aufgrund von Mangel an betrieblichen Systemen kann hier verstärkend wirken. Seien Sie auch bei der privaten Nutzung aufmerksam, um unangenehme Folgen für sich und Ihre Familien zu vermeiden. Bitte beachten Sie, besonders in diesen für uns alle herausfordernden Zeiten, die folgenden Sicherheitshinweise:

Sicherheitsempfehlungen für die E-Mail-Nutzung:

- **Vorsicht bei E-Mails** von unbekannten Adressen, die z. B. Links mit Informationen zu aktuellen Themen enthalten (z. B. Schutzmasken, Desinfektionsmitteln oder Video-Konferenzen).
- **Klicken Sie nicht** auf den verdächtigen Link und öffnen Sie auf keinen Fall entsprechende Anhänge.
- Führen Sie **Downloads** immer nur aus den **Originalquellen** und entsprechend der **intern geltenden Vorgaben** durch.
- Seien Sie grundsätzlich **misstrauisch**, wenn Sie **persönliche Daten** übermitteln sollen.
- Seien Sie skeptisch, wenn der Absender **keine Absende-Adresse des genannten Unternehmens** nennt, die Absende-Adresse fehlerhaft ist oder es sonstige Auffälligkeiten gibt.
- Prüfen Sie **Text** der E-Mail und die **Signatur** des Absenders.
- Wurde die E-Mail bereits durch das System als **auffällig** klassifiziert?
- Unterhalten Sie überhaupt eine **Geschäftsbeziehung** zum Absender?
- Bei **persönlicher Anrede:** überprüfen Sie, ob Sie den Absender kennen und woher er Ihre Daten hat.

So erkennen Sie Fakeshops:

- Die **Preise für die Ware** sind außerordentlich **niedrig** und können nur per **Vorauszahlung** bezahlt werden.
- Begehrte Produkte sind **permanent verfügbar**.
- Der Onlineauftritt ist **unvollständig** und/oder **fehlerhaft.**

- Teile der Internetseiten beinhalten **keinen Inhalt**.
- Impressum, Datenschutzerklärung, Allgemeine Geschäftsbedingungen **fehlen** oder sind fehlerhaft.
- Der Anbieter ist Ihnen **nicht bekannt** und es fehlen Erfahrungswerte, auch von anderen Nutzern.

Bitte melden Sie Verdachtsfälle umgehend Ihrem/Ihrer Administrator/-in, Informationssicherheits- oder Datenschutzbeauftragten.

Hier ein Beispiel der letzten Tage: