

## QGroup präsentiert » Best of Hacks«: Highlights Oktober 2020

Frankfurt am Main, 19. November 2020 – Cybersecurity und Datenschutz werden immer wichtiger: Kürzlich verstarb in Düsseldorf eine Frau auf dem Weg in ein weiter entfernt gelegenes Krankenhaus, da die näher gelegene Notaufnahme mit Ransomware zu kämpfen hatte. In Finnland landeten im Oktober tausende Patientenakten in den Händen skrupelloser Erpresser.

Das finnische **Psychotherapiezentrum Vastaamo**, mit rund 18.000 Patienten und Filialen in 24 Orten, wurde Opfer eines Hackerangriffs. Es wurden private Daten aus Psychotherapie-Sitzungen von mehr als 10.000 Patienten gestohlen. Den Betreibern der Klinik sowie in der Folge auch deren Patientinnen und Patienten wurde per E-Mail mit der Veröffentlichung dieser Daten gedroht. Die Hacker versuchten auf diese Weise Geld zu erpressen. Als keine Zahlung erfolgte, wurden im Tor-Netzwerk Daten von mehreren hundert Personen veröffentlicht.

Die MySQL-Datenbank der Wordpress-basierten Info-Webseite zum besonderen elektronischen Anwaltspostfach (BeA) der **Bundesrechtsanwaltskammer** wurde scheinbar von einer Ransomware-Gang gelöscht. Auf dem Server läuft eine aus dem Internet erreichbare MySQL-Installation, in die man sich ohne Benutzernamen und Passwort einloggen kann. In beiden Datenbanken auf dem Server befindet sich nur noch eine Tabelle mit der Mitteilung, dass man eine Onion-Webseite im Tor-Netzwerk aufrufen und dort einen Code eingeben soll, wenn man seine Daten wiederhaben möchte. Ruft man diese Seite auf, wird man aufgefordert, 0,06 Bitcoin zu überweisen. Die Bundesrechtsanwaltskammer bestreitet bis dato den Vorfall. Die Webseiten der Bundesrechtsanwaltskammer und die BeA-Subdomain wurden allerdings zwischenzeitig auf einen neuen Server umgezogen.

Die **Software AG** mit Sitz in Darmstadt wurde Opfer eines Malware-Angriffs. Interne Systeme wurden daraufhin kontrolliert heruntergefahren. Dennoch ist es unbekanntem Angreifern gelungen, Mitarbeiterdaten von Servern und Notebooks zu erbeuten. Unbekannt ist, ob auch Kundendaten von dem Datendiebstahl betroffen sind.

Der französische IT-Dienstleister **Sopra Steria** wurde Opfer der Ransomware „Ryuk“. In Paris befindliche Windows-Server wurden angegriffen und Datenträger im Netzwerk teilweise verschlüsselt. Das genaue Ausmaß des Angriffs ist unbekannt. Betroffen sei allem Anschein nach auch der Active Directory-Domänencontroller des Unternehmens, heißt es.

(2.369 Zeichen)

### Medienkontakt:

QGroup GmbH  
Berner Straße 119  
60437 Frankfurt am Main  
www.qgroup.de/presse

Lars Bothe  
Tel.: +49 69 17 53 63-014  
E-Mail: l.bothe@qgroup.de