

PRESSEMITTEILUNG

Angst vor Corona öffnet Datenklau Tür und Tor: So schützen sich Verbraucher und Mitarbeiter

Hannover, 8. April 2020. Die Corona-Krise führt zu einem deutlichen Sicherheitsrisiko für die IT von Verbrauchern und Unternehmen. Wie das auf Datenschutz, Informationssicherheit und IT- Compliance spezialisierte Unternehmen Althammer & Kill mitteilte, ist eine veränderte Vorgehensweise der Täter bei sogenannten Phishing-Mails und Fake-Shops zu verzeichnen. Die Täter nutzen die Angst vor COVID-19 aus, um User zu Klicks auf gefährliche Links zu verleiten, falschen Überweisungen oder Bestellungen auszuführen. Für umfassende Informationen rund um Datenschutz in Zeiten von Corona, hat Althammer & Kill die Seite www.corona-datenschutz.de ins Leben gerufen.

Cyber-Kriminelle verbreiten Viren, Erpressungssoftware (Ransomware) und Verschlüsselungstrojaner oder versuchen, an persönliche Daten zu gelangen. „Das ist ein erhebliches Sicherheitsrisiko nicht nur für Verbraucher, sondern besonders auch für die IT-Infrastruktur von Unternehmen“, weiß Thomas Althammer, Geschäftsführer von Althammer & Kill. „Mit einem Klick auf den falschen Link werden die sensiblen Daten auf dem eigenen Rechner ausgespäht; auch das Lahmlegen ganzer Systeme samt Lösegeldforderungen ist keine Seltenheit.“ Die Angriffe durch Cyber-Kriminelle sind teilweise aufwendig vorbereitet. Mitarbeiter*innen und Verbraucher*innen sollten sensibilisiert und geschult werden, um Sicherheitsrisiken zu minimieren. Es ist empfehlenswert, Verdachtsfälle umgehend dem Informationssicherheits- oder Datenschutzbeauftragten zu melden.

5 Tipps für mehr Datensicherheit

1. **Absende-Adresse checken:** E-Mails von unbekanntem, unvollständigen oder fehlerhaften Adressen mit Links zu aktuellen Themen wie Schutzmasken oder Desinfektionsmitteln löschen.
2. **Kein Klick, kein Problem:** Verdächtige Links nicht anklicken, keine Anhänge öffnen.
3. **Keine persönlichen Daten preisgeben:** Misstrauen ist gefragt, wenn persönliche Daten zur Übermittlung von Informationen abgefordert werden. Dies gilt auch bei verdächtigen Telefonanrufen.

4. **Unbekannte Online-Shops überprüfen:** Der Shop ist unbekannt, die Preise außerordentlich niedrig? Es lohnt ein Blick in Impressum, Anschrift, AGBs.
5. **Bekannter Absender, verdächtiger Inhalt:** Auch bei vermeintlich bekannten Absendern lohnt sich eine Prüfung. Der angezeigte Name und die dahinterliegende E-Mail-Adresse müssen nicht identisch sein!

Dieses Vorgehen nutzen Cyber-Kriminelle in der Corona-Krise

Phishing-Mails sind Versuche, über gefälschte E-Mails an persönliche Daten des Internet-Nutzers zu gelangen oder ihn zu einer bestimmten Aktion zu verleiten. Oft wird Druck durch Fristsetzung aufgebaut oder mit einem besonders lukrativen Geschäft gelockt.

Bei der sogenannten CEO-Fraud sollen Firmen z. B. zu Zahlungen manipuliert werden. Dazu werden falsche Identitäten genutzt. Hier werden Entscheidungsträger zum Beispiel aufgefordert, Lieferungen wie Schutzmasken oder Desinfektionsmittel zeitnah im Voraus zu bezahlen.

Bei „Fake Shops“ werden relevante und derzeit kaum verfügbare Produkte angeboten. Dabei handelt es sich um Nachbauten existierender Online-Shops oder in Betrugsabsicht aufgebaute Web-Präsenzen von Unternehmen, die gar nicht existieren. Die Lieferung wird durch den Kunden bezahlt aber nicht zugestellt.

Aufgrund der konspirativen Vorgehensweise durch Täter und die Möglichkeiten zur Anonymisierung im Internet gestaltet sich die Strafverfolgung dieser Täter schwierig und überwiesene Beträge sind häufig nicht zurückzuerhalten. Die Täter beziehen die hohen Belastungen von Mitarbeitern in der aktuellen Situation bewusst in ihre Tatvorbereitung ein.

„Die außerordentlich hohe Stressbelastung darf nicht zu einem Rückgang der Security-Awareness und des Gefahrenbewusstseins innerhalb der Belegschaft führen“, rät Althammer deshalb seinen Kunden.

Über Althammer & Kill:

Die Althammer & Kill GmbH & Co. KG hat sich als Beratungsunternehmen auf die Themen Datenschutz, Informationssicherheit und IT-Compliance spezialisiert. Zum 30-köpfigen Team gehören Juristen, IT-Berater, zertifizierte Datenschutzbeauftragte

und IT-Sicherheitsspezialisten. Das Unternehmen ist von den Standorten Hannover, Düsseldorf und Mannheim aus bundesweit tätig, z. B. in der Funktion als externe Datenschutzbeauftragte oder Informationssicherheitsbeauftragte. Zu den weiteren Angeboten zählen die Bereiche Zertifizierung und die Durchführung von IT-Sicherheitsanalysen/Penetrationstests.

Kontakt:

Susanne Maack
Pressereferentin

Mail: sm@althammer-kill.de
Mobil: 0170 933 17 52

Althammer & Kill GmbH & Co. KG
Roscherstraße 7
30161 Hannover