Cyber Crime | Achtung vor neuen Betrugsmaschen während der Corona-Krise

Als wären die gegenwärtig zu bewältigenden Herausforderungen der Corona-Pandemie für jeden Einzelnen, Gesellschaft, Staat und Unternehmen nicht schon groß genug, sind derzeit verstärkt cyberkriminelle Tätigkeiten und neue Formen von Betrugsmaschen zu beobachten. Egal ob klassische Phishing-Mails mit Corona-bezogenem Inhalt oder eine neue Form der Fake-President-Angriffe: Cyberkriminelle versuchen gerade auch in Krisenzeiten Sicherheitslücken und Unachtsamkeit gnadenlos auszunutzen. Es ist also erhöhte Vorsicht geboten.

Achtung: Phishing-Mails mit neuem Inhalt

Cyberkriminelle nutzen derzeit das verstärkte Informationsbedürfnis nach aktuellen Informationen zur Ausbreitung des Corona-Virus, um ihre Schadsoftware in täuschend echte E-Mails zu verpacken, die vorgeben, aktuelle Fallzahlen darzustellen oder nützliche Gesundheitstipps und Sicherheitsmaßnahmen zu enthalten. Wird auf den entsprechenden Link geklickt oder der angehängte Inhalt geöffnet, ist das Gerät regelmäßig mit Malware infiziert. Aber auch andere klassische Betrugsmaschen, wie das Abfragen von Zugangsdaten mittels gefälschter Login-In-Masken, wurden schon mit Corona-Bezug identifiziert.

Zu den unschönen und gefährlichen Folgen zählen unter anderem mittels Trojaner-Programmen abgefangene Passwörter, gekaperte Laptops oder sogar Schadsoftware, die Festplatten verschlüsselt und für deren Freigabe Zahlung von Lösegeld gefordert werden. Gerade jetzt, wo viele Mitarbeiter im Home Office arbeiten, sinkt im heimischen Umfeld unter Umständen die Achtsamkeitsschwelle beim Öffnen von E-Mails. Zudem ist die IT-Sicherheitsinfrastruktur vieler Unternehmen derzeit durch die externen Zugriffe der Mitarbeiter besonders gefährdet.

Achtung: Neue Form der Fake-President-Angriffe / CFO Fraud

Der zuletzt erfolgte Ausbau von Vertretungsregelungen bei Zahlungsfreigaben aufgrund der Corona-Krise lockt ebenfalls Betrüger an. Zusätzlich sind Abstimmungen zwischen Kollegen im Home Office umständlicher bzw. aufwändiger. Cyber-Kriminelle nutzen durch geschickt eingefädelte Anrufe die bisher fehlende Routine neuer Vertreter, um die Freigabe von Zahlungen außerhalb der üblichen Standardprozesse zu erzwingen.

Das kleine Einmal-Eins der Achtsamkeit

- Doppelte Vorsicht beim Öffnen von Links oder Anhängen in E-Mails unbekannter Absender oder bei Eingabe von Login- oder Verifizierungs-Daten auf Websites, die über E-Mail-Links aufgerufen werden
- Genaue Überprüfung der Absenderadresse bei vermeintlich bekannten Kontakten
- Verwenden sicherer Passwörter, regelmäßige Softwareupdates und aktiver Virenschutz
- Keine telefonische Auskunft ggü. vermeintlichen Vertretern von Banken, Gesundheits- oder Sicherheitsbehörden und Finanzämtern
- Telefonische Rücksprache mit dem Vorgesetzen zur Prüfung der erhaltenen Freigabe

Sofortmaßnahmen

- Sensibilisierung und Hinweis der Mitarbeiter auf die aktuelle Gefährdungslage mittels Rundschreiben oder Veröffentlichungen im Intranet
- Empfehlungen, Checklisten o.ä. zur Eindämmung von Risiken
- Online-Schulungen mit Tipps zur Absicherung der Kommunikationswege

Beim Ergreifen wirksamer Sofortmaßnahmen stehen Ihnen unsere erfahrenen Berater gerne mit Rat und Tat zur Verfügung.

Bei Fragen zum Thema Datenschutz und IT-Sicherheit im Home Office verweisen wir auf unsere beiden Newsletter "Home Office während der Corona-Krise – was aus datenschutzrechtlicher Sicht jetzt zu beachten ist" und "Home Office und IT-Sicherheit – Was gilt es zu beachten? Welche Sofortmaßnahmen gibt es?"

Ihre Ansprechpartner

Dirk Seeburg, M.A.E.S. (Basel), LL.M.
Rechtsanwalt

Technopark II | Werner-von-Siemens-Ring 12
85630 Grasbrunn | Germany

Tel. +49 (89) 90 420 49-62
Fax +49 (89) 46 14 90-78
Mobil +49 (170) 913 76 17

dirk.seeburg@bay-gmbh.com

Tobias Baader, M.Sc.

Luitpoldpark | Uferweg 11
88131 Lindau | Germany

Tel. +49 (8382) 27 30 79-21
Fax +49 (8382) 27 30 79-30
Mobil +49 (170) 888 60 84

tobias.baader@bay-gmbh.com