Zwei Drittel wollen angesichts der Crowdstrike-Panne einen IT-Notfallplan entwickeln bzw. den bestehenden nachbessern oder haben das bereits getan. BSI-Präsidentin Claudia Plattner unterstreicht die Relevanz solcher Maßnahmen: "Die vorliegenden Umfrageergebnisse zeigen, dass eingeübte IT-Notfallkonzepte wichtiger Bestandteil jeder Krisenvorsorge sein müssen!"

Hinweis: Das BSI unterstützt Maßnahmen zur Erhöhung der Cybersicherheit mit Info-Materialen sowie Informationen zu Initiativen und Netzwerken [LINK]

9 Warnmeldungen des BSI in den XXX Ausgaben des Buerger-Cert-Newsletters: SICHER INFORMIERT

1 Warnung vor Quishing

Die Polizei warnt aktuell vor dem sogenannten ***Quishing***. Bei dieser Betrugsmasche kommen QR-Codes zum Einsatz, die beispielsweise per Briefpost versendet werden. Wer den QR-Code scannt, um zum Beispiel die persönlichen Daten zu aktualisieren, wird auf eine gefälschte Webseite geleitet. Die dort eingegebenen Daten fallen Cyberkriminellen in die Hände

Quelle: Polizei Köln LINK
Fundort: Buerger-Cert-Newsletters: SICHER • INFORMIERT Nr. 20-.2024 vom 26.09.2024
Weiterführende *Hinweise* des LKA NRW LINK

2 Deutscher Linux-Entwickler wird Swatting-Opfer

Beim sogenannten ***Swatting*** senden Täterinnen und Täter absichtlich einen falschen Notruf ab, um Polizei oder Spezialeinheiten (bzw. SWAT-Teams) zu einem ahnungslosen Opfer zu schicken. Swatting wird oft im Zusammenhang mit Online-Gaming sowie von Akteuren in den sozialen Netzwerken genutzt, um Menschen einzuschüchtern oder bloßzustellen. Jüngstes Opfer: René Rebe, CEO des Berliner Softwareunternehmens Exactcode GmbH, der während eines Livestreams von der Polizei verhaftet wurde. Rebe kritisierte im Anschluss, dass die Ermittlungsbehörden die angeblich von ihm verfasste Drohmail nicht ausreichend auf Echtheit geprüft hätten.

Quelle: Golem LINK
Fundort: Buerger-Cert-Newsletters: SICHER • INFORMIERT Nr. 20-.2024 vom 26.09.2024
Weiterführende Hinweise des BSI zu LINK

3 Sorge vor neuartiger Android-Malware

Eine neue Malware namens ***NGate*** kann es Kriminellen ermöglichen, an Geldautomaten unautorisierte Geldabhebungen zu tätigen. Die Betrüger nutzen dazu verschiedene Phishing-Techniken, um eine bösartige App auf den Android-Geräten ihrer Opfer zu platzieren und sie mit der NGate-Malware zu infizieren. Die Malware kann Daten von NFC-fähigen Bankkarten auslesen und an die Angreifer weiterleiten.

Quelle: Chip.de LINK
Fundort: Buerger-Cert-Newsletters: SICHER • INFORMIERT Nr. 20-.2024 vom 26.09.2024

4 Doppelte Vorsicht bei Temu

Bei einem Hack sind angeblich Datensätze von 87 Millionen Kundinnen und Kunden des chinesischen Online-Marktplatzes gestohlen worden. Den Angreifern zufolge werden die erbeuteten Daten aktuell über das Darknet-Forum BreachForums zum Verkauf angeboten. Temu dementiert. Nutzerinnen und Nutzer sollen auf Nummer sicher gehen und ihr Benutzerkonto per Zwei-Faktor-Authentisierung absichern.

Quelle: Heise Online LINK
Fundort: Buerger-Cert-Newsletters: SICHER • INFORMIERT Nr. 20-.2024 vom 26.09.2024
Weiterführende Hinweise des BSI zum Account-Schutz LINK