2020-012 CERT-Hessen Warnmeldung

03.04.2020 Bearbeiter: Wiegand

Betrugsversuche im Kontext der Corona-Krise

Tags: Corona, Phishing, Fake-Shops, Betrug

Sachverhalt:

das Hessen CyberCompetenceCenter und die hessische Polizei beobachten verstärkt Betrugsversuche und Versuche zur Verbreitung von Schadsoftware im Kontext der Corona-Pandemie.

Firmen wie Privatpersonen erhalten in großem Umfang E-Mails, die auf staatliche Corona-Soforthilfen hinweisen sowie stark nachgefragte und schwer erhältliche Waren wie Schutzmasken, Desinfektionsmittel und Corona-Schnelltests bewerben. Dabei wird auf Fake-Shops, eBay und ähnliche Dienste oder Webseiten verlinkt, die Schadsoftware verteilen. In vielen Fällen sind diese Angebote nicht seriös; die Opfer werden betrogen oder mit Schadsoftware angegriffen.

Darüber hinaus versuchen Angreifer Ihre Opfer mit vermeintlich geheimen oder konkreten, ortsbezogenen Informationen mit Corona-Bezug zum Öffnen von Dateianhängen oder Links, die Schadsoftware verbreiten, zu verleiten. Auch die verstärkte, oftmals spontan ermöglichte Nutzung von Telearbeit ist mit zusätzlichen Risiken verbunden.

Gleichzeitig wurden im Rahmen des Pandemie-Managements sehr schnell Kapazitäten erweitert oder neue geschaffen. Unabhängige Studien und Auswertungen des Bundesamtes für Sicherheit in der Informationstechnik deuten darauf hin, dass dabei oft Sicherheitsaspekte zurückgestellt oder vernachlässigt wurden. Dies schafft zusätzliche Angriffspunkte, nach denen Cyberkriminelle derzeit gezielt suchen.

Bewertung

Erfolgreiche Angriffe mit Schadsoftware können zu erheblichen Störungen des medizinischen Betriebs führen.

Empfehlung von Maßnahmen

Das Hessen Cyber Competence Center empfiehlt:

- Sensibilisieren Sie alle Beschäftigten, weisen Sie auf das besondere Risiko hin
- Öffnen Sie keine Links in unverlangt zugesandten E-Mails
- Überprüfen Sie vor dem Aufruf von Links diese mit Hilfe von Suchmaschinen
- Bestellen Sie keine Waren in Internetshops, die Sie nicht kennen
- Seien Sie misstrauisch, wenn Vorkasse verlangt wird (Bezahlung vor Lieferung)

- Folgen Sie bitte keinen Links, die auf angeblich aktuelle, ortsbezogene Listen oder Karten mit Corona-Infizierten verweisen
- Informieren Sie sich bitte ausschließlich bei seriösen Anbietern (wie z.B.: BEHÖRDEN, der HKG, dem RKI oder den Angeboten des öffentlich-rechtlichen Rundfunks)

Sollten Sie im Rahmen der Pandemie-Maßnahmen ad hoc-Lösungen im IT-Bereich realisiert haben (z.B.: für die Einwahl von Mitarbeitern aus dem home-office, neue Webseiten) empfiehlt das Hessen3C, die Sicherheit dieser Lösungen nachträglich zu überprüfen und ggfs. nachträglich zu verbessern.

Im Dokument https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf <https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/empfehlung_home_office.pdf> finden Sie zahlreiche Hinweise zur sicheren Ausgestaltung der Tele-Arbeit.

Bei Cyber-Angriffen oder zur Klärung von Verdachtsfällen steht Ihnen die Hotline des Hessen CyberCompetenceCenter unter 0611-353-9900 rund um die Uhr zur Verfügung.

.

Ihr CERT-Hessen

Kurzfassung: Bedeutung der Traffic Light Protocol-Einstufungen

TLP-Stufen

Stufe	Bedeutung	Bestimmungen
TLP-White	**Unbegrenzt**	Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP-White ohne Einschränkungen frei weitergegeben werden.
TLP-Green	**Organisations-übergreifende Verteilung**	Informationen in dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Information darf jedoch nicht veröffentlicht werden.
TLP-Amber	**Organisationsinterne Verteilung**	Informationen in dieser Stufe dürfen innerhalb der Organisationen der Empfänger weitergegeben werden, jedoch nur auf der Basis „Kenntnis nur wenn nötig". Der Ersteller der Information muss zusätzlich beabsichtigte Einschränkungen der Weitergabe klar spezifizieren.
TLP-Red	**Persönlich, nur für benannte Empfänger**	**TLP-Red-Informationen** sind auf den Kreis der Anwesenden in einer Besprechung oder einer Video-/Telefonkonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. In den meisten Fällen werden Informationen der Stufe TLP-Red mündlich oder persönlich übergeben.

Eine ausführliche Erläuterung zum Traffic-Light-Protokoll finden Sie im Dokument „CERT-Verpflichtung-TLP.pdf" unter http://www.cert.hessen.de

Kontaktdaten:

Hessen CyberCompetenceCenter
CERT-Hessen

Hessisches Ministerium des Innern und für Sport
Friedrich-Ebert-Allee 12
65185 Wiesbaden

Telefon, Hotline 24/7: +49 (611) 353 9900
E-Mail: cert-hessen@hmdis.hessen.de
Website: http://www.cert.hessen.de/