PRESSEMITTEILUNG

German Competence Centre
against Cyber Crime e. V.

Verschärfte Gefahrenlage der IT-Sicherheit durch COVID-19

Aufgrund der aktuellen Ausgangslage der Homeoffice-Regelungen ausgelöst durch COVID-19 wird die bisherige Gefahrenlage in der IT-Sicherheit zusätzlich strapaziert. Das German Competence Center against Cyber Crime sieht die wesentlich gestiegene Gefahr einer Zunahme von Cybercrime. Durch bestehende Schwachstellen und weitere Kommunikationswege kann die bisherige IT-Sicherheit zusätzlich durch DDoS-Angriffe, Ransomware oder Phishing strapaziert werden.
Der gemeinnützige Verband informiert über die Bedrohungslage und Schutzmöglichkeiten. Das G4C-Mitglied Link11 bietet zudem kostenlose IT-Sicherheit für den öffentlichen Sektor an.

Wiesbaden, 30. März 2020 – Das German Competence Centre against Cyber Crime e. V. (G4C) warnt davor, dass die COVID-19-Pandemie aktuell zahlreiche Cyberkriminelle auf den Plan ruft. Eine besonders große Gefahr für Unternehmen und auch Privatpersonen geht von unterschiedlichen Angriffsarten auf das Netz aus. Beispiele hierfür sind die sogenannte Ransomware, aber auch Distributed-Denial-of-Service-Angriffe (DDoS) oder Phishing. Der Verband, der sich aus Mitgliedern der Wirtschaft sowie staatlichen Institutionen wie dem Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammensetzt, stellt hier ein neu aufgelegtes Informationsangebot rund um Ransomware zum Download zur Verfügung. Die neue Broschüre hilft Unternehmen und Institutionen, das Phänomen der Festplattenverschlüsselung samt Lösegelderpressung besser zu verstehen, gibt mit Checklisten Tipps zur Prävention und spricht Handlungsempfehlungen für den Ernstfall aus.

Ransomware in der Corona-Krise: das Geschäft mit der Angst

Cyberkriminelle Angreifer versuchen in der weltweiten Krise, den akuten Informationsbedarf der Bevölkerung zu kapitalisieren. „Das geschieht momentan insbesondere mittels Spam-Mails von scheinbar offiziellen Stellen mit angeblichen Ratschlägen zum Umgang mit dem Corona-Virus, die unsichere Links oder schadhafte Anhänge beinhalten“, erklärt Peter-Michael Kessow, Geschäftsführer des G4C. „Aber auch Fake-Shops im Internet mit in der Krise stark nachgefragten Waren wie Mundschutz oder Desinfektionsmitteln sowie interaktive Karten über die Verbreitung des Corona-Virus werden von den Kriminellen genutzt, um User zum fatalen Klicken zu verleiten.“ Werden diese von Betroffenen angeklickt oder geöffnet, im Falle der Pandemie-Karte sogar heruntergeladen, kann sich ein Trojaner wie Emotet ausbreiten und weitere Schadsoftware wie die sogenannte Ransomware nachladen.

Unsere Partner

Bundeskriminalamt

Bundesamt
für Sicherheit in der
Informationstechnik

PRESSEMITTEILUNG

German Competence Centre
against Cyber Crime e. V.

Kostenloser DDoS-Schutz für den öffentlichen Sektor

Gefährlich sind auch DDoS-Angriffe auf besonders wichtige Institutionen, die sich um die Gesundheit der Bevölkerung kümmern. Bei der derzeitigen Belastung wäre es erschreckend, wenn die Versorgung durch Attacken auf das Netz der Organisationen lahmgelegt würde.
Deshalb werden die Mitglieder des Vereins in der Krise ebenfalls für mehr Sicherheit aktiv: Der deutsche IT-Sicherheitsanbieter Link11 stellt allen Einrichtungen des öffentlichen Sektors seine Schutzlösungen bis September 2020 kostenfrei zur Verfügung. Das Angebot richtet sich an öffentliche Gesundheitseinrichtungen, Behörden sowie Bildungsträger, diese können sich gegen gezielte Überlastungen ihrer IT-Systeme durch DDoS-Attacken schützen lassen. Details zu diesem Angebot hat Link11 auf seiner Webseite veröffentlicht.

Gleichzeitig stellt G4C eine Checkliste zum sicheren Homeoffice Arbeitsplatz zur Verfügung, um Unternehmen und Nutzern dieser Regelung aktiv zu unterstützen und ein starker Partner in schwierigen Zeiten zu sein. Diese Checkliste können Sie per E-Mail über folgende Adresse anfordern: info@g4c-ev.org.

Weitere Informationen zu G4C, seinen Mitgliedern und der Vereinsarbeit stehen auf der neu gelaunchten Website www.g4c-ev.org zur Verfügung.

Über G4C

Als gemeinnütziger Verein hat sich das German Competence Centre against Cyber Crime (G4C) zum Ziel gesetzt, präventiv, ermittelnd und reaktiv gegen Angriffe im Cyberraum vorzugehen. G4C fungiert so als Know-how-Träger, Frühwarnsystem und Initiator eines regelmäßigen Austauschs über Bedrohungen aus dem Netz. Operative Kooperationspartner sind das Bundeskriminalamt (BKA) und das Bundesamt für Sicherheit in der Informationstechnik (BSI). Darüber hinaus besteht auch international ein Informationsaustausch mit relevanten Stellen zur Bekämpfung von Cyberangriffen (z. B. USA: National Cyber-Forensics and Training Alliance-NCFTA, Großbritannien: Cyber Defence Alliance-CDA).

Die Arbeit des Vereins basiert auf vier Säulen: G4C baut sukzessive eine aktuelle Datenplattform neben dem direkten persönlichen Austausch als Frühwarnsystem aus, übernimmt Datenausleitungen für das BKA und andere Ermittlungsbehörden, und engagiert sich in der Aus- und Fortbildung sowie bei Zuverlässigkeitsüberprüfungen zur Kompetenzstärkung von Cybersicherheitsbeauftragten. Gründer und Initialmitglieder von G4C sind Banken und Versicherungen; der Verein weitet seine Kompetenz jedoch konsequent auf weitere Branchen aus.

Unsere Partner

Bundeskriminalamt

Bundesamt
für Sicherheit in der
Informationstechnik

Pressekontakt
Julia Gerecht
Tel: +49 69 92010-161
presse@g4c-ev.org

German Competence Centre
against Cyber Crime e. V. (G4C)
Borsigstraße 36, 65205 Wiesbaden