

Pressemitteilung

Bundeslagebild Cybercrime 2018: Weiterhin enger Austausch von Unternehmen im Kampf gegen Cyberkriminalität notwendig G4C erwartet steigende Bedrohung durch Ransomware

Wiesbaden, 19. November 2019 – Wirtschaftsunternehmen verzichten nach wie vor auf die Anzeige von Cybercrime-Vorfällen. Beweggrund dafür sind unter anderem potenzielle Reputationsschäden. Zu dieser Erkenntnis gelangt das Bundeskriminalamt (BKA) im [Bundeslagebild Cybercrime 2018](#), an dessen Erstellung das German Competence Centre against Cybercrime e.V. (G4C) beteiligt war. „Dieser Verzicht auf eine Anzeige erschwert es Behörden und Vereinen wie G4C gleichermaßen, neue Entwicklungen im Bereich der Internetkriminalität frühzeitig zu identifizieren“, erklärt Peter-Michael Kessow, Geschäftsführer von G4C.

Damit sowohl Präventions- als auch Ermittlungsmethoden weiterentwickelt werden können, spielt der Informationsaustausch jedoch eine zentrale Rolle. „Betroffene Unternehmen können sich auch als Nicht-Mitglieder zum Beispiel an G4C wenden, sodass auf diesem Weg andere potenzielle Opfer informiert werden können“, so Kessow. Die Mitglieder von G4C tauschen sich kontinuierlich und vertraulich über aktuelle Bedrohungsszenarien und Cybervorfälle aus und suchen in akuten Fällen nach geeigneten Lösungen. Der Austausch sowie die enge Zusammenarbeit mit den G4C- Kooperationspartnern Bundeskriminalamt und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) stellen dabei die Weichen für Maßnahmen der Gefahrenabwehr und Strafverfolgung.

Ein Phänomen, das die Behörden, G4C und seine Mitglieder weiterhin besonders beschäftigt, sind Angriffe mit sogenannten Erpressungs-Trojanern (engl. Ransomware). Die Täter verschlüsseln per Software die IT-Infrastruktur ihrer Opfer. In Folge dessen fordern sie hohe Lösegeldzahlungen für die Freigabe der Daten; von einer Zahlung raten Behörden und G4C jedoch im Normalfall ab. In 2018 sank laut BKA-Lagebilds zwar die Gesamtzahl der Ransomware-Angriffe, es standen allerdings vermehrt Unternehmen im Fokus der Angreifer. Im Jahr 2019 beobachten G4C und seine Mitglieder bisher, dass die Gesamtzahl der Ransomware-Angriffe sowie dadurch verursachte Schäden wieder steigen. „Die Täter verlagern ihre Aktivitäten zunehmend auf lukrativere Geschäftsfelder und professionalisieren dafür ihr

Vorgehen“, erläutert G4C-Geschäftsführer Kessow diesen Trend. Kleine und mittlere Unternehmen sind hiervon betroffen, da ihre IT-Systeme im Vergleich zu großen Firmen tendenziell weniger gegen die sich stetig weiterentwickelnde Cyberkriminalität geschützt sind. Doch auch immer mehr große Unternehmen oder zentrale Dienstleister sehen sich durch diese Angriff gefährdet. Kommt es zu einer Verschlüsselung der Daten und Infrastrukturen, leisten G4C und seine Mitglieder konkrete und praktische Unterstützung bei der technischen Absicherung von betroffenen Unternehmen.

Dass Cybercrime durch Ransomware auch für den gesamten Wirtschaftsstandort Deutschland von zunehmender Bedeutung ist, zeigt eine weitere aktuelle Entwicklung in diesem Bereich. Besonders Unternehmen der kritischen Infrastruktur, wie beispielsweise Energieversorger, geraten vermehrt in den Fokus von Cyberkriminellen. Hierzu veranstalteten G4C und weitere Partner am 4. November 2019 in Berlin einen Parlamentarischen Abend. In diesem Rahmen herrschte Einigkeit bei Veranstaltern und Teilnehmern, dass es ein noch engeres Kooperationsnetz gegen derartige Ransomware-Angriffe geben muss. Peter-Michael Kessow begrüßt dieses Fazit: „Das zeigt uns, dass die enge Partnerschaft zwischen G4C und seinen Mitgliedsunternehmen sowie den Behörden BKA und BSI ein sinnvoller und zukunftsfähiger Ansatz im Kampf gegen Cyberkriminalität ist.“

Eine neue Veröffentlichung von G4C zum Cybercrime-Trend Ransomware kann in der G4C-Geschäftsstelle per Mail (info@g4c-ev.org) oder telefonisch (06122 17848-00) angefordert werden.

Über G4C

Als gemeinnütziger Verein hat sich das German Competence Centre against Cybercrime (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.

Pressekontakt

German Competence Centre against Cybercrime e.V. (G4C) / Pressestelle

c/o A&B One, Julia Gerecht, Tel 069 / 920 10-135, presse@g4c-ev.org

Seite 2 von 3

German Competence Centre against Cybercrime e.V. (G4C)

Pressestelle

069 / 920 10-135

presse@g4c-ev.org