German Competence Centre
against Cybercrime e.V.

GEMEINSAM STARK

CYBERSICHERHEIT
FÜR UNTERNEHMEN UND BEHÖRDEN

Strategie und Organisation

Analyse

www.g4c-ev.org

Prävention

Schadensbegrenzung

Abwehr

Aufklärung

Frühwarnsystem

Forschung

Austausch

Unsere
Kooperationspartner

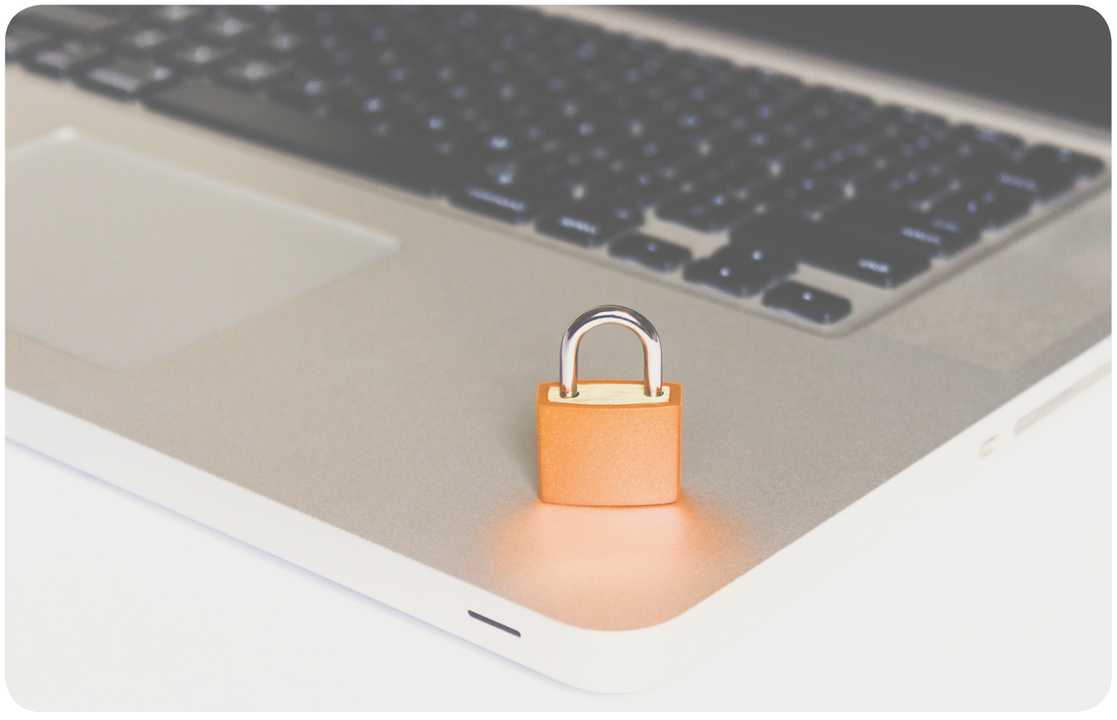
Bundeskriminalamt

Bundesamt
für Sicherheit in der
Informationstechnik

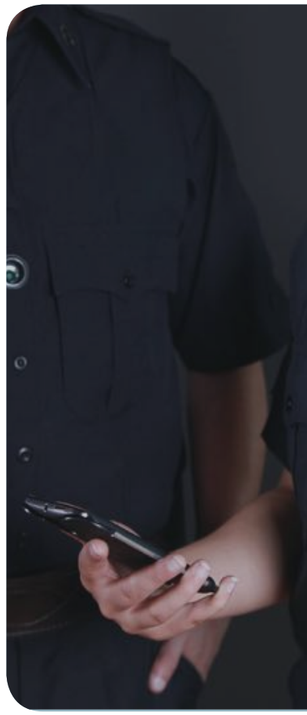
Sicherheit im Cyberraum

“Das Thema Informations- und Cybersicherheit hat branchenübergreifend enorm an Bedeutung gewonnen. Grund dafür ist die hochgradige Vernetzung aller Geschäftsprozesse. Das technische Spezialwissen und die vernetzten Abläufe sind für den Anwender nicht mehr komplett zu erfassen. Deshalb ist es notwendig, dass hochspezialisierte Teams interdisziplinär zusammenarbeiten. Das tun wir bei G4C.”

Roland Wolf, Vorstand des G4C



Inhalt



GEMEINSAM STARK GEGEN CYBERCRIME

Sehr geehrte Damen und Herren,

Sie werden das Thema in den Nachrichten verfolgt haben: Internetkriminalität oder auch Cybercrime stellt eine immer größere Bedrohung dar. Nicht nur für Privatpersonen oder Großkonzerne, sondern auch für kleine und mittelständische Firmen, für Versorgungs- und Infrastruktureinrichtungen. Und das geht ebenfalls immer wieder durch die Medien: Die Gefahr dieser virtuellen Kriminalität wird nach wie vor von vielen Unternehmen unterschätzt.

Bei allen Chancen, die die digitale Vernetzung von Mensch, Maschine, Prozessen und Plattformen bietet, beinhaltet sie jedoch auch extrem vielfältige und in Einzelfällen sogar existenzbedrohende Risiken. Der Diebstahl von Kunden- und Lieferantendaten sowie anderer sensibler Geschäftsgeheimnisse verursacht ebenso wie die Störung von Produktionsprozessen die Gefahr hoher Kosten und – und dies ist vielleicht noch gravierender, weil nur langfristig zu beheben – die Gefahr von Reputationsschäden.

Mit der Einrichtung des German Competence Centre against Cybercrime e. V. (G4C) haben sich Unternehmen der verschiedensten Branchen in Deutschland zusammengeschlossen, um der Internetkriminalität mit präventiven Abwehrmaßnahmen entgegenzuwirken.

Exklusiv unterstützt wird der Verein vom Bundeskriminalamt (BKA) und dem Bundesamt für Sicherheit in der Informationstechnik (BSI). Der vertrauensvolle Informationsaustausch innerhalb des Vereins hat zum Ziel, dass sich Systemfehler oder Anwenderprobleme in den Mitgliedsunternehmen nicht wiederholen. Bei Erkennen von u.a. neuen Cybercrime Phänomenen und Trends, sowie neuen Schwachstellen und Bedrohungen, werden die Behörden auch von sich aus aktiv und informieren das G4C und seine Mitglieder über angemessene und erfolgskritische Abwehrmaßnahmen. So können wir im Regelfall sogar proaktiv Schäden größeren Ausmaßes verhindern.

Diese resultieren oftmals daraus, dass Cybercrime-Angriffe zu spät erkannt werden. Dabei ist eine zeitnahe Reaktion auf Cybercrime-Vorfälle ein entscheidender Faktor, um drohende unternehmerische Schäden einzudämmen. Das Wissen um die eigene Situation – welche Maßnahmen zur Sicherung der Systeme gibt es, wo bestehen Lücken, wo kann die Sicherheit noch verbessert werden – ist ein entscheidender Vorsprung im Angesicht dieser Bedrohungslage. Wir bieten Ihnen an, eine entsprechende Analyse bei Ihnen durchzuführen, um Sie zu stärken gegen die Gefahr durch Cyberkriminelle.

Ich würde mich sehr freuen, wenn Sie eine solche Risikoeinschätzung in Anspruch nehmen und uns die Gelegenheit zu einem vertiefenden Gespräch im Anschluss geben würden. Gerne würde ich Sie dann auch über weitere Einzelheiten zu unserem Verein informieren.

In der Hoffnung, Ihr Interesse geweckt zu haben, verbleibe ich

mit freundlichen Grüßen

Roland Wolf,
Vorstandsvorsitzender

Wiesbaden, Oktober 2019

Borsigstr. 34, 65205 Wiesbaden

Entstehungsgeschichte des G4C e. V.

ZIELSETZUNG

- Prävention, Detektion und Reaktion
- individueller Kontakt der Privatwirtschaft zu den Sicherheitsbehörden in unterschiedlicher Ausprägung
- Aufklärung und Gegenmaßnahmen durch Sicherheitsbehörden im internationalen Verbund
- Zeitnahe, gebündelte Intelligence und Fallzusammenführung

2011

- Bedarf einer institutionalisierten Zusammenarbeit von Privatwirtschaft und Sicherheitsbehörden
- erster Institutional Public Private Partnership-Workshop, initiiert und organisiert durch das BKA

2012

- Klärung verschiedener Zusammenarbeitsmodelle und Anforderungen
- Informationsaustausch mit National Cyber-Forensics und Training Alliance (NCFTA)

VEREINSGRÜNDUNG

Als gemeinnütziger Verein mit Sitz in Wiesbaden hat das G4C e.V. zum 01.01.2014 seine operative Arbeit aufgenommen.

Gründungsmitglieder sind drei Unternehmen aus der Finanzbranche (Commerzbank, ING und HypoVereinsbank), die je ein Mitglied des Vorstands stellen.

2013

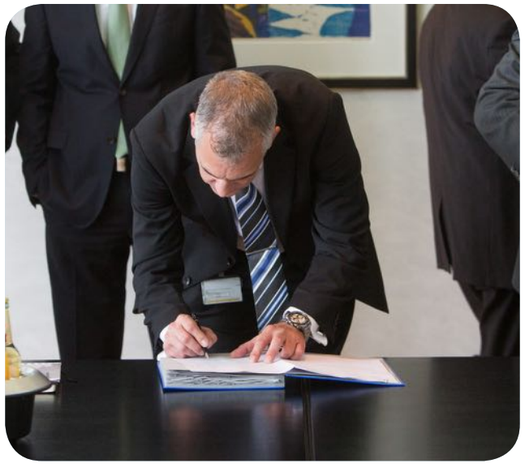
- Start der Gründungsvorbereitung und Abgabe einer Absichtserklärung zur Vereinsgründung
- Erstellung Satzung und Beitragsordnung
- Erstellung einer detalierten Kooperationsvereinbarung mit dem BKA
- Gründungsversammlung

NEUAUFSTELLUNG DES VEREINS

Weiterentwicklung der Geschäftsstelle zur Verstärkung der Mitarbeit innerhalb des Vereins sowie Intensivierung der Kommunikation mit fachlichen Partnern.

2018

- Einsetzung eines Geschäftsführers
- Wachstum des Vereins über den Finanzsektor hinaus
- Weiterentwicklung und Vermarktung des Produktportfolios



Verein

Als eigenständiger, operativ tätiger, gemeinnütziger Verein ist G4C Know-how-Träger, Frühwarnsystem und Informationsplattform.

Der Verein sorgt dafür, dass Mitglieder und Kooperationspartner ihre Erkenntnisse über aktuelle Bedrohungen austauschen.

Die operative Leistungsfähigkeit und die branchenübergreifende Vernetzung unterscheiden den Verein von existierenden Netzwerken und Allianzen zum Thema Cyberkriminalität. Sie machen ihn zum wertvollen und wichtigen Partner der Wirtschaft im deutschen und internationalen Immunsystem gegen Cyberkriminalität.

Das größte Unterscheidungsmerkmal zu existierenden Netzwerken und Allianzen ist der enge und tägliche Informationsaustausch zwischen den Kooperationspartnern und den Mitgliedern des Vereins. Zu diesem Zweck arbeiten Vereinsmitglieder und Partner gemeinsam unter einem Dach.

Die Arbeit des Vereins ist effizient, weil er Akteure aus unterschiedlichen Bereichen der Prävention in einer strategischen Allianz zusammenbringt. So werden Wissen, Kompetenz und Erfahrung gebündelt und für alle Mitglieder und Partner praktisch nutzbar.

G4C ist sehr daran interessiert, weitere Kompetenzträger auf dem Feld der Cyberkriminalität zusammenzubringen. Ein Ziel des Vereins ist es, das Netzwerk zur Prävention zu erweitern. Durch Aufnahme weiterer Unternehmen möchte G4C die Expertise des Vereins zur Prävention gegen Cyberkriminalität entlang der gesamten Wertschöpfungskette im Online-Handel stärken.

von links nach rechts:
Heiko Wolf (Vorstand G4C) und Andreas Lüning (Vorstand G DATA)
bei der Unterzeichnung der Aufnahmebestätigung in Bochum

Unsere Ziele

Übergreifende Analyse der Cyberkriminalität, Feststellung von Modi Operandi

Erarbeitung präventiver Schutzmaßnahmen

Schaffung einer Austauschplattform über alle Branchen hinweg

Initiierung und Durchführung von Studien, Kampagnen und Forschungsprojekten

Vorstand

Roland Wolf

1. Vorsitzender/Finanzen

Roland Wolf, gelernter Bankkaufmann, wechselte nach 15 Jahren im Investmentbanking in den IT-Bereich. Seit 2001 begleitet er bankintern das Thema IT-Sicherheit und betreut seit 2008 das Thema Konzernsicherheit in der Commerzbank.

Heiko Wolf

2. Vorsitzender/Öffentlichkeitsarbeit

Heiko Wolf verfügt über eine langjährige Erfahrung im Bereich IT-Sicherheit/-Governance und arbeitet seit 1996 im IT-Umfeld von Banken und Wirtschaftsprüfern. Aktuell ist er Leiter des Ressorts Information Risk Management der ING und betreut die Themen Informationssicherheit, Business Continuity, Management sowie personelle und physische Sicherheit.

Tibor Konya

3. Vorsitzender/Organisation und Entwicklung

Tibor Konya war bis 2012 nach einer zunächst behördlichen Tätigkeit im Sicherheitsbereich für die Corporate Security eines großen Industrie-unternehmens tätig. Im Anschluss wechselte er zur UniCredit Bank AG. Dort verantwortet er neben Information Security die Felder Business Continuity, Management und Security Intelligence.

Unser Team

Geschäftsführung

Peter-Michael Kessow

Managing Director, Security Consultant

Langjährige Führungskraft bei der Bundespolizei, zuletzt Vizepräsident des Präsidiums Ost in Berlin.

Kontakt

Tel.: +49 (0)6122 178 4800
E-Mail: P.Kessow@g4c-ev.org

Projektleitung und Organisation

Ingmar Weitemeier

Vertretung der Geschäftsführung, Projektleitung

Direktor des Landeskriminalamtes a. D.

Kontakt

Tel.: +49 (0)6122 178 4800
Mobil: +49 (0)172 450 9625
E-Mail: I.Weitemeier@g4c-ev.org

Joachim Hock-Tessmann

Externer Berater Projekte Controlling

Kontakt

Tel.: +49 (0)6122 178 4800
Mobil: +49 (0)176 517 97 425
E-Mail: J.Hock-Tessmann@g4c-ev.org

Security Consulting

Dr. Kai Buchholz-Stepputtis

Principal Security Consultant

Kontakt

Tel.: +49 (0)6122 178 4800
Mobil: +49 (0)172 66 03 809
E-Mail: K.Buchholz-Stepputtis@g4c-ev.org

Unsere Mitglieder

“Das Vertrauen in Unternehmen ist für eine funktionierende Wirtschaft ebenso unerlässlich wie das Vertrauen zwischen Unternehmen und seinen Kunden. In der zunehmend vernetzten Welt kommt der Sicherheit im Cyberspace eine wachsende Bedeutung zu. Der gemeinsame Austausch im G4C-Mitgliederkreis ist wichtig, um Entwicklungen früh zu erkennen und Lösungen zum Schutz zu etablieren.”

Christian Funk
Leiter Information Security
SCHUFA Holding AG

COMMERZBANK

ING Die Bank und Du

HypoVereinsbank UniCredit Group

KFW Bank aus Verantwortung

R+V DIE VERSICHERUNG MIT DEM PLUS

schufa

Symantec.

G DATA SIMPLY SECURE

LINK 11

bank-verlag

DIEBOLD NIXDORF

Unsere Kooperationen

Institutionalisierte Zusammenarbeit von Privatwirtschaft & Sicherheitsbehörden

Bundeskriminalamt

Bundesamt für Sicherheit in der Informationstechnik

Das Thema Informations- und Cybersicherheit wird für Unternehmen immer wichtiger. Gründe dafür sind die hochgradige Vernetzung der Geschäftsprozesse und die damit einhergehende Abhängigkeit von funktionierenden IT-Systemen.

In den letzten Jahren hat die Anzahl und die Qualität von Cyberangriffen kontinuierlich zugenommen. Und damit auch die Gefahr, dass diese Angriffe erfolgreich sind.

Prävention von Cyberkriminalität funktioniert deshalb nur in Kooperation. Hier unterscheidet sich G4C von anderen existierenden Netzwerken und Allianzen.

Der Verein arbeitet mit hochspezialisierten Teams aus dem BKA und dem BSI interdisziplinär zusammen. Vereinsmitglieder und Partner arbeiten gemeinsam unter einem Dach.

Der Verein bündelt Wissen, Kompetenz und Erfahrung und macht sie für seine Mitglieder praktisch nutzbar. Die Kooperation mit dem BKA und dem BSI ermöglicht dabei schnellen und effektiven Informations- und Wissenstransfer zu potenziellen Bedrohungen.

G4C und seine Mitglieder erarbeiten in Kooperation mit dem BKA und BSI Präventionsmaßnahmen, die den Schutz der IT der Unternehmen verbessern und die Gefahr von illegalen Angriffen minimieren.

v.l.: Heiko Löhr (BKA), Ingmar Weitemeier (G4C) und Stefan Methien (BKA)

Unsere Kooperationspartner

BUNDESKRIMINALAMT

Das Bundeskriminalamt ist die Zentralstelle der deutschen Polizei mit der Aufgabe, die nationale Kriminalitätsbekämpfung in enger Zusammenarbeit mit den Landeskriminalämtern zu koordinieren Das Bundeskriminalamt verfügt in bestimmten schwerwiegenden Kriminalitätsfeldern über eigene Ermittlungskompetenzen, insbesondere auch bei länderübergreifenden und internationalen Zusammenhängen. Das gilt für besondere Fälle der Cyberkriminalität, die vielfach enorme Schäden herbeiführen, Handlungsmöglichkeiten von Unternehmen erheblich einschränken oder gar eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen verursachen können.

Somit gehört die Cyberkriminalität zur schweren und organisierten Kriminalität. Auch staatliche Stellen sind aufgerufen, dieser Form der Kriminalität nicht nur im Bereich der Strafverfolgung, sondern auch im Bereich der Prävention mit hoher Priorität entgegenzutreten. Im Bewusstsein, dass dies nicht ohne Beteiligung der Wirtschaft erfolgreich geschehen kann, hat das Bundeskriminalamt frühzeitig die Zusammenarbeit mit geeigneten Kooperationspartnern gesucht.

Deshalb haben sich die Verantwortlichen des Bundeskriminalamtes am 21. Januar 2014 entschlossen, mit dem gemeinnützigen Verein G4C, der eine Reihe von Wirtschaftsunternehmen als Mitglieder zählt, eine Kooperation zum Schutz der Allgemeinheit einzugehen.

An diesem Tag unterzeichneten der Vizepräsident des Bundeskriminalamtes, Prof. Dr. Jürgen Stock, sowie die Vorsitzenden des Vereins G4C eine Vereinbarung über die Kooperation im Phänomenbereich Cyberkriminalität.

Das BKA sorgt dafür, dass wichtige Erkenntnisse, die für die Mitgliedsunternehmen von großer Bedeutung zur Sicherung ihrer IT sind, möglichst schnell an potentielle Opfer herangebracht werden und somit sehr hohe Schäden vermieden werden können. Gleichzeitig ist die Behörde auch sofort ansprechbar, wenn es um rechtswidrige Angriffe auf Netze der Mitgliedsunternehmen geht. Sofern erforderlich können sehr schnell Ermittlungsmaßnahmen zur Strafverfolgung in Gang gesetzt werden. Das schützt gleichzeitig auch andere gefährdete Mitgliedsunternehmen. Durch die Kooperation mit dem G4C leistet das BKA auf dieser Plattform durch die Besprechung von Lösungen zu aktuellen und zukunftsorientierten Themen seinen Beitrag zur Prävention bzw. Bekämpfung von Cybercrime.

Dazu sitzt Fachpersonal des Bundeskriminalamtes bei G4C mit am Tisch, wenn es um den Austausch aktueller Informationen geht, um die Gefahren für Unternehmen zu minimieren. Somit können – in Ergänzung der Maßnahmen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) – durch diese Kooperationen Gefahren ohne Zeitverlust adressiert, abgewehrt und Schäden verhindert werden.

Die bisherige Kooperation hat den Mehrwert sichtbar deutlich gemacht.

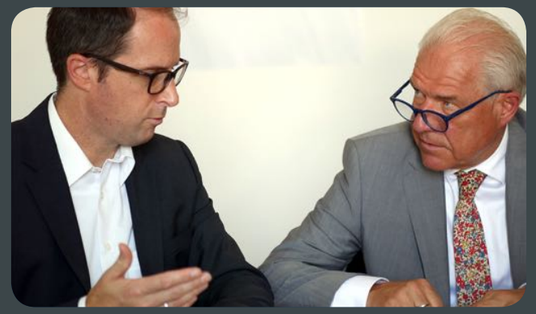
von links nach rechts:
Jan Hendrick Peters (BSI),
Peter M. Kessow (G4C),
Vizepräsident Dr. Gerhard Schabhüser (BSI)
und Michael Dwucet (BSI)
bei einem Kooperationstreffen in Bonn

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK

Am 22.01.2015 haben das G4C e.V. und das Bundesamt für Sicherheit in der Informationstechnik (BSI) einen Kooperationsvertrag unterzeichnet. Inhalt der Kooperation ist die gemeinsame Prävention gegen Cyberkriminalität.

„Cyberkriminalität stellt eine große Herausforderung für Unternehmen dar, ganz besonders für die Finanzbranche. Durch die Kooperation mit dem BSI als nationaler IT-Sicherheitsbehörde können wir den Austausch von Wissen zu neuen Bedrohungen künftig noch weiter verbessern“, erklärte Roland Wolf, erster Vorsitzender des Vereins.

Der Informationsaustausch zu aktuellen Bedrohungsszenarien ist auch in den Augen von BSI- Vizepräsidenten Dr. Gerhard Schabhüser ein wichtiger Bestandteil der Prävention gegen die zunehmenden Aktivitäten von Cyberkriminellen: „Cyberangriffe auf Unternehmen finden jeden Tag mit zunehmender Professionalität und Zielrichtung statt. Um angemessene Schutzmaßnahmen entwickeln zu können, dürfen diese Angriffe von den Betroffenen nicht verschwiegen, sondern müssen in einem vertrauensvollen Umfeld diskutiert werden.“



v.l.: Heiko Löhr (BKA) und Ingmar Weitemeier (G4C)

v.l.: Ingmar Weitemeier (G4C), Vizepräsident Peter Henzler (BKA) und Peter M. Kessow (G4C)

G4C-Vorstand bei einem Kooperationstreffen

Vertragsunterzeichnung beim G4C e.V.

Kooperation mit dem Bundeskriminalamt

Kontinuierlicher gemeinsamer Informationsaustausch über die Entwicklungen

In Anbetracht der überdurchschnittlich großen Anzahl von Cybercrime-Straftaten, die bei der Polizei nicht zur Anzeige gebracht werden (Dunkelfeld), werden zur umfassenden Einschätzung der Gefahrenpotentiale von Cybercrime auch Erkenntnisse von nichtpolizeilichen Informationsquellen in die polizeiliche Lagebeurteilung miteinbezogen. Einen intensiven Austausch gibt es mit G4C.

Die auf diesem Wege gewonnenen Informationen ergänzen das polizeiliche Hellfeld des BKA und ermöglichen eine qualitativ verbesserte Lagebewertung, die weitergehende und zielorientierte Präventionsmaßnahmen ermöglichen.

Die Expertise des G4C wird auch genutzt, um die polizeiliche Perspektive mit der des G4C anzureichern und in aktuellen Lagebildern des BKA Bewertungen des G4C mit einzuarbeiten.

G4C Mitglieder geben zum Beispiel bedeutsame Aussagen zu Phänomen wie Ransomware.

Im Jahr 2018 gab es zwar einen Rückgang von 20 % im Gesamtbereich der Ransomware, allerdings ist die Anzahl der angewandten Varianten, die gezielt Unternehmen angreifen, um 12 % gestiegen. G4C beobachtet im Jahr 2019 allerdings wieder verstärkt Angriffe mit Ransomware.

Die Zahlen und Entwicklungen belegen eine weiter zunehmende Bedrohung für die Wirtschaft und sprechen für ein gezielteres und professionalisiertes Vorgehen der Cyberkriminellen, die ihre Aktivitäten in „lukrativere“ Geschäftsfelder verlagern.

Laut G4C-Mitglied Symantec belegt Deutschland in Bezug auf die Häufigkeit von Infizierungen durch Mobile Ransomware den dritten Platz hinter den USA und China.

….zu Phänomenen wie DOS-Angriffen

Nach Informationen von G4C-Mitglied Link 11 haben DOS-Angriffe im Jahr 2018 an Qualität und Quantität stark zugenommen. Im Gegensatz zu 2017 ist 2018 ihre Anzahl nicht nur um 34 % angestiegen, sondern es erhöhte sich auch die durchschnittliche Angriffsbreite derartiger Attacken von 1,7 Gbit/s auf 4,9 Gbit/s, wodurch ein schnellerer Kollaps angegriffener Organisationen erreicht wurde.

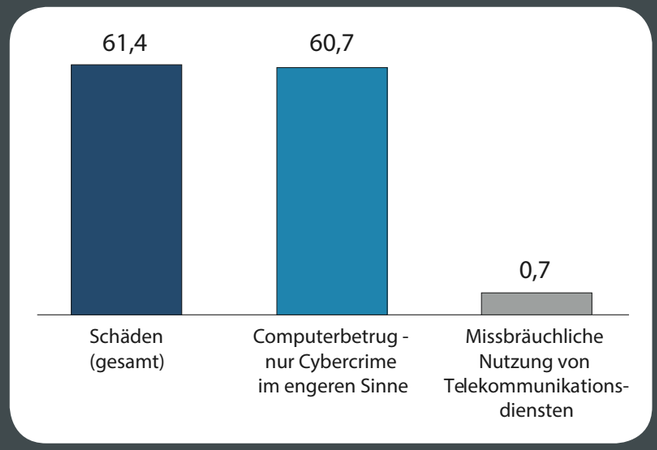
…..zu Phänomenen wie mobile Malware

Das G4C-Mitglied G-Data berichtet, dass insbesondere Android-Nutzer betroffen sein sind. Im Durchschnitt verzeichnete G-Data 11.700 neu-identifizierte Mobile Malware für Android pro Tag, somit alle acht Sekunden eine neue Malware. Es werden allerdings auch vermehrt IOS-Endgeräte von Malware jeder Art geschädigt.

Die Anzahl der im Jahr 2018 neu programmierten Malware-Varianten bezifferten sich allein für Android-Geräte auf ca. 4,1, Mio. – ein Zuwachs von knapp 27 % im Vergleich zum Vorjahr.

AKTUELLE PHÄNOMENE

Quelle:
Bundeskriminalamt



SCHÄDEN DURCH CYBERCRIME IN MIO. EURO (2018)

Quelle:
Bundeskriminalamt

Portfolio

CDCH: Compromised Data Clearing House

Die kommerzielle Seite des Internets wird auch von Kriminellen verwendet. In Internetforen oder auf Handelsplattformen tauschen sie sich über Modus Operandi aus oder bieten gehackte oder gestohlene Daten (Kreditkartendaten, Accountdaten, Bankdaten etc.) an. Das BKA erlangt in unregelmäßigen Abständen Zugriff auf solche Plattformen und somit auch Zugriff auf die Daten der Opfer, die es zu verarbeiten gilt.

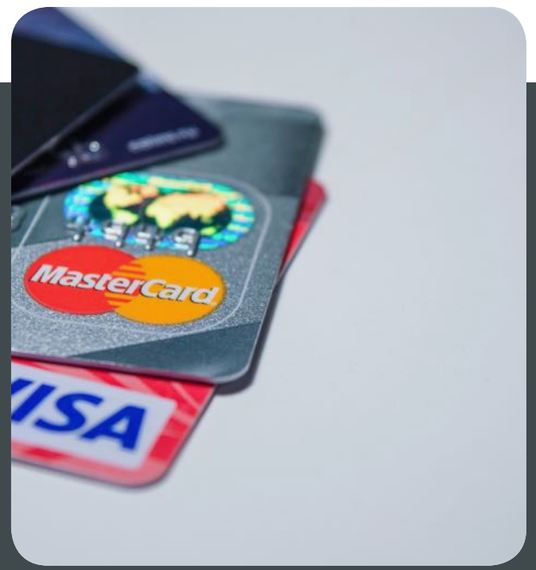
Deswegen wird das G4C von der Staatsanwaltschaft beauftragt, persönliche Daten von Kunden an die entsprechenden Unternehmen auszuleiten, damit diese in der Lage sind, sich und ihre Kunden vor weiteren Schäden zu schützen. Damit ermöglicht die Datenverarbeitung eine intensive Zusammenarbeit mit dem BKA.

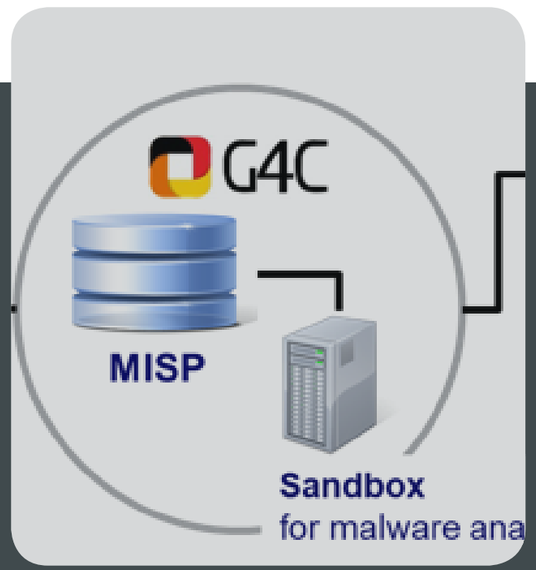
MISP: Malware Information Sharing Plattform

Jeden Tag untersuchen IT-Forensiker komplexe Bedrohungen der IT-Infrastruktur. Die Aufgabe der Experten besteht im Zusammenstellen verschiedener Fragmente zu einem zusammengehörigen Ganzen. Diese können aus einfachen Metadaten oder aus komplizierten und bösartigen Codes bestehen. Diese Beschreibung wird Indicator of Compromise (IOC) genannt.

IOCs beschreiben somit im besten Falle Wie, Wann und Wo sowie Warum ein Angriff auf die IT stattfindet. Damit gehört der IOC zur wichtigsten Dokumentation eines IT-Sicherheitsexperten.

Mit dem Teilen und Verbreiten solcher Informationen auf Sharing-Plattformen partizipieren die Teilnehmer von den unterschiedlichen Herangehensweisen und Wissensständen der Anderen. Diese Plattformen dienen somit dem Wissenstransfer und der Schärfung von IOC.





DUEN: Darknet Underground Economy

Mitgliedsunternehmen von G4C haben im November 2017 damit begonnen, das Darknet nach strafrechtlich relevanten Sachverhalten bzw. Vorbereitungshandlungen zu durchsuchen. Das geschieht unter maßgeblicher fachlicher und methodischer Anleitung durch das BKA/SO 4 sowie der Prüfung der rechtlichen Zulässigkeit durch die Generalstaatsanwaltschaft Frankfurt am Main und mit der Zustimmung des G4C-Vorstandes.

Die damit verbundenen Abläufe wurden in einem Prozesshandbuch festgehalten. Ziel der Maßnahme ist das rechtzeitige Erkennen bestehender sowie künftiger Ereignisse mit Bedrohungspotenzial für die Mitgliedsunternehmen des G4C.

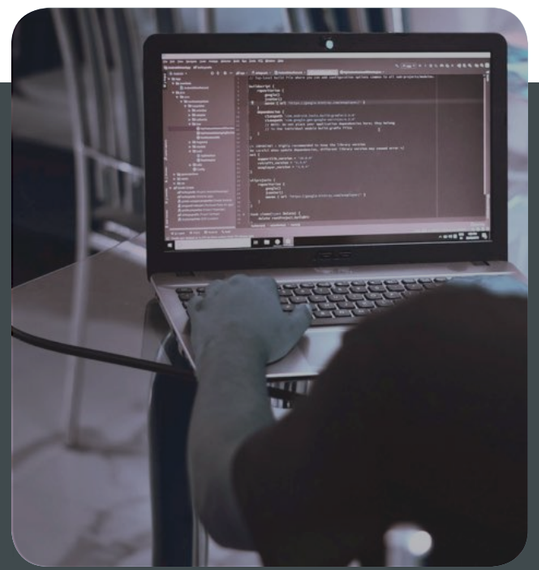
Konkret sollen aus der Underground Economy und dem Darknet Informationen über die Mitgliedsunternehmen, Schadsoftware, geplante und in Planung befindliche DDoS Attacken, APTs, etc. erkannt und zum Schutz der Unternehmen analysiert werden.

Sicherheitsüberprüfungen

Aufgrund der Tatsache, dass nicht nur die Technik Schwachstellen aufweist, sondern auch die handelnden Personen nicht immer vertrauenswürdig sind, setzt sich das G4C auch mit dem Thema Sicherheitsüberprüfungen/Zuverlässigkeitsüberprüfungen auseinander.

Es kommt darauf an, vor Einstellungen in Unternehmen, aber auch nach gewissen Zeitabständen, Mitarbeiter, die an sensiblen Schnittstellen arbeiten (Vorstände/IT-Mitarbeiter) auf ihre Integrität zu überprüfen.

Dabei sind die taktischen Möglichkeiten vielfältig. Besonders zu beachten ist allerdings, dass die Maßnahmen rechtmäßig sind und bleiben Diese Rechtmäßigkeit kann sich aus Spezialgesetzen (z.B. AtomG, GWG) ergeben. Sollte es keine spezielle gesetzliche Regelung vorhanden sein, so ist auf die arbeitsrechtlichen Normen zurückzugreifen. Diese schränken die durchführbaren Möglichkeiten im Rahmen der Verhältnismäßigkeit ein.
G4C gibt auch hier weitergehende Lösungsansätze und Hinweise.



Unser Informationsmaterial für Unternehmen

Zielscheibe Unternehmen: Ransomware

Das Thema der Verschlüsselungstrojaner hat den erwarteten und vorausgesagten Schritt in seiner Evolution genommen: die sogenannte Ransomware wird nun auch ganz gezielt gegen Unternehmen ausgebracht. Lösegeldforderungen in Bitcoins sind nicht mehr nur zufällig und pauschal, sondern richten sich jetzt auch mit bis zu siebenstelligen Eurobeträgen am betroffenen Unternehmen aus.

Damit die Täter solche hohen Summen fordern können, bemühen sie sich, die Ransomware im gesamten Netzwerk des Unternehmens zu verbreiten. Ziel ist, möglichst große Teile der Datenbestände (einschließlich des Back-ups) des Unternehmens zu verschlüsseln und damit lahmzulegen.

Gelingt dies, kann das Unternehmen im „worst case" vor der unangenehmen Alternative Totalverlust oder Eingehen auf die Lösegeldforderungen stehen.

Damit die G4C-Mitgliedsunternehmen in Kundengesprächen das Thema Ransomware zeitnah und effektiv kommunizieren können, hat ein G4C-Team eine Unternehmensbroschüre zur diesem Thema erstellt.

Damit sollen die Unternehmen zu diesem zunehmenden und hochgefährlichen Phänomen sensibilisiert werden, sowie wichtige Hinweise zu verbesserter Prävention und Detektion, aber auch Hilfestellungen für den eingetretenen Fall erhalten. Die Broschüre ist über G4C zu erhalten.

Unternehmen und Institutionen als (ganz gezielte) Zielscheibe von Ransomware

Zielscheibe Unternehmen: CEO-Fraud

Unternehmen stehen zunehmend im Visier von Cyberkriminellen. Zunächst werden Firmen hierbei über das Internet ausspioniert. Im Anschluss steht ein Mitarbeiter im Mittelpunkt des Täter-Interesses. Der Mitarbeiter wird geschickt manipuliert und gibt vielfach arglos vertrauliche Daten des Unternehmers preis oder weist Zahlungen an Fremdkonten an.

Das typische Vorgehen bei „CEO-Fraud" besteht darin, dass zahlungsberechtigte Mitarbeiter (z. B. aus der Buchhaltung) gefälschte Nachrichten vom vermeintlichen Chef/Geschäftsführer/CEO des Unternehmens erhalten. In diesen Nachrichten gibt er dem betreffenden Mitarbeiter den Auftrag hochvertrauliche Finanztransaktionen durchzuführen. Als Gründe werden z. B. Firmenübernahmen, Strafzahlungen o. ä. angeführt, demgemäß ist der „ganz persönliche Auftrag aus der Chefetage" natürlich streng geheim. Fällt der betroffene Mitarbeiter auf dieses „Social Engineering" herein, können im Anschluss Schäden in bis zu zweistelligen Millionenbeträgen entstehen.

Die Strategien der Angreifer sind vielfältig. Allen gemein ist, dass menschliche Eigenschaften, wie zum Beispiel Hilfsbereitschaft, Vertrauen, Angst oder Respekt vor Autorität ausgenutzt werden. Mitarbeiter werden so manipuliert, dass sie gutgläubig handeln und dabei das eigene Unternehmen unbewusst schädigen.

In einer Broschüre des Bankenverbands, an der G4C-Mitgliedsbanken maßgeblich beteiligt waren, erfahren Unternehmen, wie sie sich gegen CEO-Fraud und damit verwandte Betrugsmethoden schützen können.

CEO-Fraud

G4C ist als Netzwerker bekannt und erfolgreich

Teilnahme an Konferenzen

Die Verantwortlichen von G4C sind gefragte Mitgestalter von Konferenzen und Veranstaltungen zum Thema Cybersicherheit. Eine besonders enge Kooperation führt G4C mit dem Behördenspiegel durch. Bei der PITS 2019 (Fachkonferenz Deutschlands für IT- und Cybersicherheit bei Staat und Verwaltung) haben Peter-Michael Kessow und Ingmar Weitemeier als Diskussionsleiter und kompetente Gesprächspartner teilgenommen. Dadurch wird nicht nur die Leistungsfähigkeit von G4C sichtbar, sondern der Austausch führt zu neuen Präventionsinitiativen.

Kooperation mit BBH

Der Geschäftsführer von G4C, Peter-Michael Kessow und Frau Prof. Dr. Ines Zenke, Partner bei der Rechtsanwaltskanzlei Becker, Büttner, Held (BBH) vereinbaren für die Zukunft eine Kooperation. Während die Erkenntnisse von G4C für BBH und ihre Mandanten von besonderer Bedeutung sind, erhalten die Verantwortlichen von G4C Zugang zu Unternehmen, die besonderes Interesse an der Abwehr von Cyberangriffen haben. Das gilt besonders für Unternehmen der kritischen Infrastruktur. Es entsteht eine vertrauensvolle Nähe zum offenen Austausch von Erfahrungen.

Kooperation mit NCFTA

Sehr viele Angriffe auf deutsche Unternehmen werden vom Ausland vorgenommen. In einer Mehrzahl von Fällen haben Täter in den USA zunächst Erfahrungen gemacht und dehnen sich dann nach Europa aus. Umso wichtiger ist eine enge Vernetzung über die Grenzen hinweg. Das geschieht nicht nur in Europa – über das Bundeskriminalamt mit Europol. G4C selbst hat eine Kooperationsvereinbarung mit der staatlichen Bekämpfungsstelle gegen Cyberkriminalität (National Cyber-Forensics and Training Alliance – NCFTA) in den USA geschlossen.

G4C unterstützt Maßnahmen zur Optimierung einer sicheren Infrastruktur

- rechtzeitige Bedrohungsinformation durch die aktive Teilnahme am “G4C investigativen Recherchenverbund” durch aktive oder fördernde Mitgliedschaft bei G4C
- Durchführung von Funktionstests der IT-Sicherheitsstruktur, IT--Organisation, Gefährdungsvorsorgeplanung
- wiederkehrende Aufklärung des Verwaltungspersonals und des technischen Leitwartenpersonals zur IT-Sicherheit
- Überprüfung der technischen/organisatorischen IT-Strukturen und der Gefahrenabwehrpläne bei Cyber Attacken

Als Betreiber einer Kritischen Infrastruktur müssen Sie angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen Ihrer IT- Systeme treffen, die für die Funktionsfähigkeit der Kritischen Infrastrukturen maßgeblich sind.

Quelle: BSI-Gesetz,
§ 8a Sicherheit in der IT
Kritischer Infrastrukturen

Analyse

Schadensbegrenzung

tion

ehr

warnsystem

Forschung

Austausch

G4C

BECKER BÜTTNER HELD

Unser Kooperationspartner ist auch die Kanzlei Becker Büttner Held, Rechtsanwälte, Wirtschaftsprüfer, Steuerberater. Diese gehört zur Unternehmensgruppe BBH, die mit ihren Gesellschaften und über 550 Mitarbeiterinnen und Mitarbeitern an sieben Standorten in Deutschland und Brüssel zu den führenden Beratern der Infrastrukturwirtschaften gehört.

Ein Großteil der 3.000 BBH-Mandanten gehört zu den Betreibern kritischer Infrastrukturen nach der BSI-Kritisverordnung aus den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit und Wasser.

Die zunehmende Cyberrelevanz von Infrastrukturwirtschaft und Daseinsvorsorge sowie der Austausch heute notwendig großer Datenmengen stellen Geschäftsleitung und Aufsichtsrat unter eine besondere Verantwortung. Deshalb berät BBH Unternehmen rechtlich, betriebswirtschaftlich, technisch und strategisch u.a. in den Themenbereichen IT-Sicherheit und Abwehr von Cyberkriminalität.

Eintrag im Vereinsregister
Wiesbaden VR 6806

www.g4c-ev.org
Stand: Oktober 2019

Bildnachweis
BS/Dombrowsky (S. 22)
Marco Urban (S. 7, 22)

KONTAKT

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

Borsigstraße 34
65205 Wiesbaden

Telefon: +49 6122 178 4800
Fax: +49 6122 178 4803
E-Mail: info@g4c-ev.org