Im Einsatz – im Thema.
POLIZEI PRAXIS

CYBERCRIME UND CYBER-SICHERHEIT IN DEUTSCHLAND:

Dr. Stefan Goertz, Bundespolizei, Hochschule des Bundes, Lübeck

Nach Angaben des Bundeskriminalamtes (BKA) ist die Bandbreite illegaler Aktivitäten und Tatgelegenheiten im Internet sehr groß und reicht von der Verbreitung von Kinderpornografie im Internet über „Phishing“ persönlicher Zugangsdaten, Handel mit Waffen und Rauschgift bis hin zu Netzwerkeinbrüchen und DDoS-Attacken, der Verbreitung von Schadsoftware und Betrugshandlungen. Cybercrime nutzt hierbei das Clearnet/Visible Web, die dort existierenden Foren der Underground Economy sowie das DeepWeb und Darknet.[1]

Cybercrime: Die Definition des Bundeskriminalamtes (BKA)
Cybercrime umfasst die Straftaten, die sich gegen das Internet, Datennetze, informationstechnische Systeme oder deren Daten richten (Cybercrime im engeren Sinne) oder die mittels dieser Informationstechnik begangen werden. Aktuell verbreitete Erscheinungsformen von Cybercrime sind gekennzeichnet durch die Infektion und Manipulation von Computersystemen mit Schadsoftware, z. B. um

- *persönliche Daten und Zugangsberechtigungen des Nutzers abgreifen und missbräuchlich nutzen zu können (Identitätsdiebstahl)*
- *darauf befindliche Daten/Dateien des Nutzers mittels sog. Ransomware zu verschlüsseln, um „Lösegeld“ zu erpressen*
- *sie „fernsteuern“ zu können, in sog. Botnetzen zusammenzuschalten und für weitere kriminelle Handlungen einzusetzen.*[2]

Cyber-Sicherheit: Die Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI)

Die Definition von Cyber-Sicherheit durch das BSI
Cyber-Sicherheit befasst sich mit allen Aspekten der Sicherheit in der Informations- und Kommunikationstechnik. Das Aktionsfeld der klassischen IT-Sicherheit wird dabei auf den gesamten Cyber-Raum ausgeweitet. Dieser umfasst sämtliche mit dem Internet und vergleichbaren Netzen verbundene Informationstechnik und schließt darauf basierende Kommunikation, Anwendungen, Prozesse und verarbeitete Informationen mit ein.[3]

Die Lage der IT-Sicherheit in Deutschland: Die Analyse des BSI

Ein wesentliches Risiko für Anwender in Staat, Wirtschaft und Gesellschaft geht nach Angaben des BSI augenblicklich von der Schadsoftware Emotet aus, die das BSI bereits im Dezember 2018 als die gefährlichste Schadsoftware der Welt bezeichnet hatte. Diese Einschätzung wurde durch die erheblichen Schäden bestätigt, die bisher durch Cyber-Angriffe mit Emotet entstanden sind. Auch unabhängig von Emotet zählt Ransomware nach wie vor zu den größten Bedrohungen für Unternehmen, Behörden und andere Institutionen sowie für

Privatanwender. Immer wieder kommt es dabei zu Komplettausfällen von Rechnern und Netzwerken, aber auch von Produktionsanlagen. Auch Einrichtungen des Gemeinwesens sind zuletzt wiederholt Ziel von Ransomware-Angriffen geworden.[4]

Die vom BSI prognostizierte neue Qualität der Cyber-Angriffe manifestierte sich durch mehrere große Fälle von Identitätsdiebstahl, die in den Jahren 2018 und 2019 für Aufmerksamkeit sorgten. Unter anderem betroffen waren Anwender von sozialen Netzwerken und Kunden einer großen Hotelkette, hunderte Prominente und Politiker aus Deutschland im Zuge des Doxing-Vorfalls, der im Januar 2019 bekannt wurde, sowie hunderte Millionen andere Internetnutzer, deren Daten im Zuge der als "Collection #1" bis "Collection #6" bezeichneten Vorfälle öffentlich im Internet verfügbar gemacht wurden. Bemerkenswert war hierbei nicht nur die Häufung der Vorfälle, sondern auch die riesige Menge der abgeflossenen und im Internet veröffentlichten persönlichen Daten.[5]

Auch in den Jahren 2018 und 2019 stellte das BSI nach wie vor eine hohe Dynamik der Angreifer bei der Entwicklung von Schadprogrammen und Angriffswegen fest. So registrierte das BSI rund 114 Millionen neue Schadprogamm-Varianten, beobachtete DDoS-Angriffe mit bis zu 300 Gbit/s Angriffsbandbreite und registrierte über 110.000 Bot-Infektionen täglich, zumeist auf mobilen Endgeräten oder Geräten des Internets der Dinge (IoT).[6]

Nach Angaben des BSI sind die Gefährdungen der IT-Sicherheit in Deutschland seit 2018 geworden. Ein Beispiel dafür sind die Hardware-Sicherheitslücken wie Spectre/Meltdown und Spectre NG. Auch wenn im Jahr 2018 neue große Ransomware-Wellen ausgeblieben sind, muss Ransomware dennoch weiterhin als massive Gefährdung eingestuft werden. Dies beweisen die Cyber-Angriffe im Jahr 2017 mit der Ransomware Petya/NotPetya, die allein in der deutschen Wirtschaft Schäden in Millionenhöhe verursachten. Seit 2018 steig die Anzahl an Schadprogrammen weiter an, so dass es im Augenblick über 800 Millionen bekannte Schadprogramme gibt und pro Tag kommen rund 390.000 neue Varianten hinzu. Im Mobil-Umfeld gibt es nach Angaben des BSI bereits mehr als 27 Millionen Schadprogramme allein für Google Android.[7]

Eine Weiterentwicklung bescheinigt das BSI auch IoT-Botnetzen. Wegen des schnellen Zuwachses an verwundbaren IoT-Geräten und Mobilgeräten sind zukünftig allerdings neue große Botnetze für wirkungsvolle Angriffe (Spam, DDoS usw.) zu erwarten. Aufgrund des Umfangs der Credential-Leaks und der Gefährdungen durch fehlkonfigurierte Cloud-Dienste gibt es auch bei Spam und Phishing keine Entspannung der IT-Sicherheitslage. Die bisher bekannt gewordenen Identitätsdiebstähle erreichen quantitativ immer neue Größenordnungen und auf dem IT-Schwarzmarkt werden zunehmend Datenkollektionen gehandelt, dabei handelt sich um Milliarden erbeuteter digitaler Identitäten.[8] Auch illegales Krypto-Mining ist seit 2018 hinzugekommen. Aufgrund der hohen finanziellen Attraktivität und der Unauffälligkeit der Infektionen bewertet das BSI Krypto-Mining als signifikant zunehmendes Cyber-Risiko. So nahmen die registrierten Vorfälle seit 2017 sowohl an Zahl als auch an Intensität zu. So war in mehreren Fällen zu beobachten, dass die Verwendung von derzeit bekannten Infrastrukturen (z. B. Botnetze und Exploit-Kits) auf die Distribution von Krypto-Currency- Mining-Malware erweitert wird.[9]

Cybercrime: Die aktuelle Analyse des Bundeskriminalamtes

Das BKA erklärt im Bundeslagebild Cybercrime 2018 – veröffentlicht am 11.11.2019 –, dass in Anbetracht der anzunehmend überdurchschnittlich großen Anzahl von Cybercrime-Straftaten, die bei der Polizei nicht zur Anzeige gebracht werde, von einem signifikanten Dunkelfeld im Bereich Cybercrime auszugehen ist.[10] Die Gründe für das vermutlich sehr große Dunkelfeld liegen nach Angaben des BKA einerseits in den Erfassungsmodalitäten, andererseits weisen die nachfolgend aufgeführten Punkte auf ein sehr hohes Dunkelfeld im Bereich Cybercrime hin:

- *Eine große Anzahl strafbarer Handlungen im Internet kommt aufgrund zunehmender technischer Sicherungseinrichtungen über das Versuchsstadium nicht hinaus und wird von den Geschädigten nicht bemerkt,*
- *Die betroffenen Personen erkennen nicht, dass sie Geschädigte einer Cyber-Straftat geworden sind (z. B. bei Diebstahl ihrer Identität bei einem Online-Shop) bzw. von ihnen eingesetzte technische Geräte unbemerkt zur Begehung von Cybercrime-Straftaten missbraucht wurden (z. B. Nutzung infizierter PCs oder Router als Teil eines Botnetzes zur Ausführung von DDoS-Angriffen oder Infektion mit Cryptomining-*

Malware),

- *Straftaten werden durch Geschädigte nicht angezeigt, insbesondere, wenn noch kein finanzieller Schaden entstanden ist (z. B. bloßer Virenfund auf dem PC) oder der eingetretene Schaden von Dritten (z. B. Versicherung) reguliert wird,*
- *Geschädigte, insbesondere Firmen, zeigen erkannte Straftaten nicht an, um bspw. die Reputation als „sicherer und zuverlässiger Partner" im Kundenkreis nicht zu verlieren.*
- *Geschädigte erstatten z. B. in Erpressungsfällen oftmals nur dann Anzeige, wenn trotz Zahlung eines Lösegelds keine Dekryptierung des durch die Täterseite zuvor verschlüsselten Systems erfolgt.*[11]

Das aktuelle Bundeslagebild Cybercrime weist für den Beobachtungszeitraum des Jahres 2018 insgesamt 87.106 Fälle von Cybercrime aus. Dabei betrug die Aufklärungsquote lediglich 38,9%. Im aktuellen Bundeslagebild registrierte das BKA insgesamt 22.051 Tatverdächtige von Cybercrime-Delikten. Aktuell haben dabei 16.832 der festgestellten Tatverdächtigen (76,3 %) die deutsche Staatsangehörigkeit, 5.219 Tatverdächtige waren Nichtdeutsche, wobei türkische (13,5 %), rumänische (9,7 %) und nigerianische (8,7 %) Staatsangehörige am häufigsten vertreten waren. Mehr als die Hälfte (58,9 %) der registrierten Delikte wurden von Tatverdächtigen begangen, die zwischen 21 und 39 Jahre alt waren. Das Täterspektrum reicht nach Angaben des BKA vom Einzeltäter bis hin zu international organisierten Tätergruppierungen. Dabei arbeiten gemeinsam agierende Täter im Bereich Cybercrime nur selten in hierarchischen Strukturen, sie kennen sich häufig nicht persönlich und nutzen auch bei arbeitsteiligem Vorgehen die vermeintliche Anonymität des Internets. Festzustellen ist, dass die Täterseite seit Jahren flexibel und schnell auf neue technische Entwicklungen reagiert und ihr Verhalten entsprechend anpasst. So werden Dienste im Bereich Cybercrime, die nicht selbst erbracht werden können, von anderen hinzugekauft (Cybercrime-as-a-Service). [12]

Folgende Phänomene beobachtet das BKA im Bereich Cybercrime unter anderem:

- Diebstahl digitaler Identitäten (ID-Theft)
  - Formjacking
  - Data Breaches
  - Doxing/Doxxing
- Phishing im Online-Banking
- Malware/Schadprogramme
  - Kryptomining
  - Emotet
- Ransomware – Digitale Erpressung
- Botnetze – Massenhafte Fernsteuerung von Computern
- DDoS-Angriffe
- Mobile Malware
- Underground Economy – Digitale Schwarzmärkte
- Digitale Währungen
- Technical Support Scams/Sextortion
- „Living-of-the-Land"/"Supply-Chain-Attacks"
- Cloud-Computing/Zunehmende Vernetzung durch das Internet der Dinge
- Maschinelles Lernen[13]

Schäden durch Cybercrime

Nach Angaben des BKA verursacht Cybercrime bei Bürgern, Behörden und Wirtschaftsunternehmen hohe materielle und immaterielle Schäden, die bis zur Existenzgefährdung reichen können. So führen millionenfacher Datendiebstahl, Manipulationen einer Vielzahl von technischen Geräten und die entsprechende Berichterstattung in den Medien zu einer deutlichen Beeinträchtigung des Sicherheitsgefühls der Bevölkerung. Einer Umfrage des BSI und des Programms Polizeiliche Kriminalprävention zufolge schätzten etwa ein Drittel der Befragten (29 %) ihre persönliche Gefahr, Opfer von Cybercrime zu werden, als hoch oder sehr hoch ein. Gemäß der ARD/ZDF-Onlinestudie von 2018 sind über 90 % der deutschen Bevölkerung (ca. 63,3 Mio. Menschen) Onlinenutzer und somit potenziell betroffen von Cybercrime. Das BKA analysiert, dass sich valide Aussagen zum tatsächlichen monetären Gesamtschaden durch Cybercrime nicht treffen lassen, weil im Lagebild Cybercrime ausschließlich

Schäden in Fällen des Computerbetrugs und der missbräuchlichen Nutzung von Telekommunikationsdiensten ausgewiesen werden. So belief sich die für das Jahr 2018 ausgewiesene Schadenssumme in diesen Bereichen insgesamt auf 61,4 Mio. Euro. Davon entfielen rund 60,7 Mio. Euro auf den Bereich Computerbetrug und knapp 0,7 Mio. Euro auf die missbräuchliche Nutzung von Kommunikationsdiensten. „Bitkom“ bemisst in einer Studie den finanziellen Schaden für die deutsche Wirtschaft durch Cybercrime für die letzten zwei Jahre auf 43,4 Mrd. Euro.[14]

Fazit

Das BKA analysiert mit fortschreitenden Entwicklungen, wie dem Internet der Dinge/Internet of Things (IoT), Industrie 4.0, „Smart Home“ oder Automotive IT (AIT) und stark zunehmenden „adressierbaren“ Objekten im Internet, dass sich das Spektrum potenzieller Ziele für Cyberkriminelle zukünftig erweitern wird. Dabei wirken sich unzureichende Absicherungen sowie veraltete Technologien kriminalitätsfördernd aus. So beinhalten die hochdynamischen Entwicklungen im Bereich der Künstlichen Intelligenz (KI) bedeutende Potenziale für die wirtschaftliche Wertschöpfung, diese bergen jedoch auch umfangreiche kriminelle Nutzungsmöglichkeiten (z. B. als „lernende Schadsoftware“). Kurz: Je umfassender sich die Gesellschaft in der digitalen Welt bewegt und je mehr Möglichkeiten diese bietet, desto mehr Tatgelegenheiten ergeben sich für Cyberkriminelle. Dies zeigt sich nicht nur an den erhöhten Fallzahlen in den letzten Jahren bei gleichzeitig niedrigerer Aufklärungsquote, sondern z. B. auch an dem massiven Anstieg der Vielfalt von Schadsoftware. So wurden im ersten Halbjahr 2018 vom G4C-Mitglied G DATA durchschnittlich ca. 13.000 völlig neu programmierte Arten bösartiger Software identifiziert werden. Das gesamte Bedrohungspotenzial Cybercrime lässt sich nach Angaben des BKA angesichts der rasanten Entwicklung und aufgrund der Tatsache, dass viele Attacken bzw. Straftaten im Dunkelfeld verbleiben, kaum abschätzen. So ist davon auszugehen, dass sowohl Fallzahlen als auch Schadenssummen sowie die Anzahl der Geschädigten weitaus höher sind, als es die polizeilichen Statistiken ausweisen.[15]

---

[1]www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html (3.1.2020).
[2] Ebd.
[3]www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/cyber-sicherheit_node.html (3.1.2020).
[4]www.bsi.bund.de/DE/Publikationen/Lageberichte/lageberichte_node.html (3.1.2020).
[5] Ebd.
[6] Ebd.
[7]www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2018.pdf (3.1.2020).
[8] Ebd.
[9] Ebd.
[10] Bundeskriminalamt (2019): Cybercrime. Bundeslagebild 2018, S. 2.
[11] Ebd., S. 5.
[12] Ebd., S. 5-8.
[13] Ebd., S. 11-48.
[14] Ebd., S. 49-51.
[15] Ebd., S. 52-53.

Alle Artikel dieser Kategorie

Datenschutz

Newsletter

Folgen Sie uns!