DIE CYBER-SECURITY-HOTLINE
0800 888 133
DER WIRTSCHAFTSKAMMERN ÖSTERREICHS

WKO.at/cys oder Cys.at und
WKO.tv/cys oder Cysec.tv

Dr. Wolfgang Schinagl

WKO Steiermark l Oktober 2019

Impressum:

Ein Produkt der WKO Steiermark.
Abteilung Technische Infrastruktur
Körblergasse 111-113, 8010 Graz
T: +43 316/601-622
E: steiermark@cys.at
W: WKO.at/cys

Graz, 16.10.2019

Idee und Start

Anfang 2017 hatte Ing. Josef Herk, Präsident der WKO Steiermark, die Idee, für die steirischen Unternehmerinnen und Unternehmer eine Cyber-Security-Hotline einzurichten. Präsident Ing. Josef Herk und Direktor Dr. Karl-Heinz Dernoscheg, MBA beauftragten den Autor mit deren Umsetzung. Der Ablauf sollte folgendermaßen aussehen: Wenn beispielsweise ein Unternehmen durch einen Ransomware-Trojaner lahmgelegt wird, ruft das Unternehmen die Notfallnummer 0800 888 133 an und erhält vom Call Center Nothilfe im Sinne einer Erstversorgung. Sollte das Problem nicht sofort gelöst werden können, wird ein Second Level mit IT-Security-ExpertInnenen/Unternehmen konsultiert. Hierfür wurde mit der WKO UBIT-ExpertsGroup IT-Security (Sprecher: DI (FH) Gerald Kortschak, BSc CMC und Mag. Harald Wenisch) ein Team von hochspezialisierten IT-SicherheitsexpertInnen-Firmen (UBIT-Mitglieder) zusammengestellt. Das Call Center erstellt Tickets und gibt diese weiter an die

1. Cyber-Security-ExpertInnen (UBIT-IT-SicherheitsexpertInnen-Firmen),
2. Projektleitung und
3. Servicecenter der WKO Landeskammern

Die Cyber-Security-ExpertInnen versuchen das Problem zu lösen. Die telefonische Erstberatung ist kostenlos, ein Einsatz vor Ort beim betroffenen Unternehmen wird firmenmäßig verrechnet. Die Cyber-Security-Hotline ist täglich von 0-24 Uhr und 7 Tage die Woche besetzt. Das Call Center führt eine Zufriedenheits- und Erfolgsmessung bei den Cybercrime-Opfern durch. Am 9.6.2017 wurde die Cyber-Security-Hotline 0800 888 133 mit einer Pressekonferenz in der WKO Steiermark gestartet.

Kommunikation der Cyber-Security-Hotline 0800 888 133

Die Website für die Cyber-Security-Hotline (abgekürzt CYS-Hotline) lautet WKO.at/cys oder cys.at. Am 15.11.2017 wurde ein eigener Cyber-Security Kanal am WKO Steiermark eigenen Internet-TV Sender: „WKO.tv Next Generation“ unter der Webadresse WKO.tv/cys oder cysec.tv gestartet. Gleich von Beginn an nahmen die Wirtschaftskammern der Bundesländer Kärnten, Burgenland, Vorarlberg, Tirol und Oberösterreich an der CYS-Hotline teil. Die Wirtschaftskammer Niederösterreich trat am 10.11.2017 der Hotline bei. Die Wirtschaftskammer Salzburg kam im 1. Quartal 2018, die Wirtschaftskammer Wien (Pressekonferenz am 3.5.2018) im 2. Quartal 2018 hinzu. Damit war eine österreichweite Ab-

deckung für Cybercrime-Notfälle bei den WKO-Mitgliedsbetrieben gegeben. Die Cyber-Security-Hotline wird auf den WKO.at Landeskammer-Seiten, in den Kammerzeitungen, Newslettern, Polizeidienststellen, Medien des Kuratoriums Sicheres Österreich (KSÖ) und österreichischen Medien kommuniziert. Beim E-Day 2018 und 2019 wurden für die Besucher Flyer und Etiketten mit der Nummer 0800 888 133 für die Bildschirmrückseite aufgelegt.

Abwicklung und Workflow

Als Call Center wurde eine Firma ausgewählt, die bereits die WKO Benutzerverwaltung unterstützt und Kompetenzen im Notfallbereich besitzt. Es wurde für den gesamten Vorgang – vom Anruf des Cybercrime-Opfers bei der Notfallnummer 0800 888 133 bis zum Abschluss der Leistung – ein Prozessablauf ausgearbeitet. Dieser Workflow beinhaltet folgende Schritte:

1. Prüfung, ob es sich um ein WKO-Mitglied handelt,
2. Fälle, die kein Notfall sind, werden ausgeschieden,
3. Telefonische Notversorgung mittels Checkliste (z.B. Anweisung zum kontrollierten Herunterfahren der Server), FAQs und Checklisten für den Cybercrime-Notfall wurde von den ExpertInnen der WKO UBIT Experts-Group IT-Security ausgearbeitet,
4. Das Call Center erstellt während des Anrufs ein Ticket und weist dem geschädigten Unternehmen eine zertifizierte ExpertIn aus der UBIT-ExpertsGroup IT-Security Liste zu, je nach geografischer Nähe zum betroffenen Unternehmen. Die Liste wird von der UBIT-ExpertsGroup IT-Security gewartet, ab Ende 2019 wird von der geografischen Zuordnung auf eine kompetenzorientierte Zuordnung umgestellt, denn jedes IT-Security-Unternehmen hat ihre spezielle Cybersecurity-Kompetenzmatrix.
5. Das Call Center informiert die AnruferIn, dass er/sie von einem IT-ExpertInnen-Unternehmen rückgerufen wird und dass die Bearbeitung des Falles über dem Ausmaß eines Informationsgesprächs kostenpflichtig ist, wobei das IT-Security-Unternehmen die Kosten selbst definiert. Der/die IT-ExpertIn finalisiert den Fall und meldet dies an das Call Center,
6. Die Dokumentation des Falls wird als Tickets dem Servicecenter der jeweiligen Landeskammer zugeordnet,
7. Das Call Center führt eine Zufriedenheits- und Erfolgsmessung durch.

Die Auswahl, Wartung und Ergänzung der IT-Security-ExpertInnen sowie die Geschäftszeiten erfolgen über die jeweiligen Wirtschaftskammer-Bundesland-

sprecherInnen in Abstimmung mit den Sprechern der WKO UBIT IT-Security ExpertsGroup. Die Entscheidung, welche neuen IT-Security-ExpertInnen auf die Liste kommen, obliegt grundsätzlich jedem Bundesland. Als Qualitätssicherheitsstandard gelten Industriezertifizierungen, hochkarätige Security-Ausbildungen wie beispielsweise der Incite-Kurs „Data & IT-Security Expert“.

Quantitative und qualitative Analyse der Service-Tickets der Cyber-Security-Hotline

Von Beginn der Cyber-Security-Hotline im 2. Quartal 2017 bis Ende 1. Quartal 2019 gingen 842 Anrufe bei der Cyber-Security-Hotline 0800 888 133 ein. Jeder Anruf wurde in einem Ticket des Call Centers erfasst. Datenschutzrechtliche Rahmenbedingungen insbesondere aufgrund der Datenschutzgrundverordnung (DSGVO) ab 25.5.2018 wurden berücksichtigt. Von diesen 842 Tickets wurden 212 Tickets an die Cyber-Security-ExpertInnen der UBIT ExpertsGroup IT-Security weitergeleitet. Die folgende Tabelle zeigt in der ersten Spalte das Bundesland, in der zweiten Spalte die Anzahl der Anrufe (Tickets), in der dritten Spalte die Summe der weitergeleiteten Tickets und in der vierten Spalte die Anzahl der Cyber-Security-Unternehmen (* Stand: September 2019). Die Tabelle ist nach der zweiten Spalte (Tickets) geordnet.

Bundesland	Tickets	Weitergeleitete Tickets	Cyber-Security-Unternehmen*
Wien	312	60	8
Oberösterreich	189	50	5
Steiermark	88	23	5
Niederösterreich	81	29	5
Tirol	66	17	5
Kärnten	32	14	7
Salzburg	32	7	5
Burgenland	23	7	4
Vorarlberg	19	5	3
Gesamt	842	212	47

Damit im Zuge einer qualitativen Analyse der Tickets festgestellt werden kann, ob die Fälle mit nationalen und internationalen Statistiken vergleichbar sind und eine ähnliche Verteilung haben, wurden die Daten mit folgenden Berichten verglichen:

1. Österreichischer Sicherheitsbericht (seit 2012 Kapitel: Cybersicherheit, seit 2015 Cyber-Security-Center),
2. Lagebericht Cybercrime 2017 des Bundeskriminalamts (BKA),
3. Cybercrime Bundeslagebild des deutschen Bundeskriminalamts (BKA) seit 2010,
4. FBI Internet Crime Complaint Centre (IC3) mit einer jährlichen Statistik seit 2002

Der Sicherheitsbericht 2017 des Bundesministeriums für Inneres (BMI) weist im Bereich Cybercrime 16.804 angezeigte Fälle (2008: 3.291 Fälle) auf, davon 3.040 Versuche, 6.470 geklärte Fälle, das ist eine Aufklärungsquote von 38,5%.

(Quelle: https://www.bmi.gv.at/508/files/SIB_2017/03_SIB_2017-Kriminalitasetsbericht_web.pdf S. B16, abgerufen am: 17.8.2019)

Cybercrime-Straftaten sind beispielsweise: der widerrechtliche Zugriff auf ein Computersystem, Internet-Nutzung als Kommunikationsplattform für Betrugsdelikte mit Tatort Internet, Kinderpornografie und die Anbahnung von Sexualkontakten zu Unmündigen (Grooming). „Die Zahl der Anzeigen von Cybercrime im engeren Sinne [Anmerkung des Autors: Straftaten, die an IT-Systemen und Daten begangen werden] ist österreichweit von 2.630 im Jahr 2016 auf 3.546 im Jahr 2017 um 34,8 % angestiegen. Gleichzeitig ist die Aufklärungsquote im Jahr 2017 um 10,2 % auf 28,2 % gestiegen. Der relativ neue § 107c StGB „Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems“ wurde im Jahr 2017 das erste Mal in dieser Statistik erfasst. Dies zeigt sowohl in der Gesamtanzahl der angezeigten Delikte als auch in der Aufklärungsquote deutliche Auswirkungen. Besonders der Tatbestand Datenbeschädigung (§ 126a StGB), mit einem Anstieg von 527 Straftaten und somit 80 %, wurde überdurchschnittlich stark angezeigt. Der Grund für diese Zunahme liegt vor allem in der weltweit steigenden Verbreitung von Ransomware. Damit werden wichtige Daten in EDV-Systemen durch einen Verschlüsselungstrojaner unbrauchbar gemacht. In der Folge versuchen die Täter für die Entschlüsselung der Daten Lösegeld in Form von Bitcoins zu erpressen. Im Jahr 2017 ist die Anzahl von Anzeigen wegen Hacking, dem unbefugten Eindringen in ein Computersystem (§ 118a StGB), um 94 Straftaten stark zurückgegangen (Rückgang von 20,6 %). Aus regionaler Sicht ist vor allem in den Bundesländern Steiermark (Plus von 38,7 %), Salzburg (Plus von 36,2%), Kärnten (Plus von 34,4 %) und Wien (Plus von 31,5 %) die Anzahl der Anzeigen von Cybercrime besonders stark angestiegen. Von den 7.448 ausgeforschten Tatverdächtigen handelt es sich um 4.067 inländische und 3.381 fremde Tatverdächtige. Letztere stammen vor allem aus Deutschland (913), Serbien (591), Tschechien (246), der Türkei (216) und der Russischen Föderation (165). Bei den Altersgruppen

sind die 25- bis 39-Jährigen mit 3.521 Verdächtigen am stärksten vertreten. In der Altersgruppe ab 40 Jahren gibt es 1.834 Verdächtige und in den Altersgruppen von 14 bis 24 Jahren sind 1.983 Verdächtige ermittelt worden, wobei in der Gruppe der besonders jungen Täter im Alter von 14 bis 17 Jahren 445 Verdächtige aufscheinen. Die Zahl der Anzeigen wegen kinderpornografischer Darstellung Minderjähriger (§ 207a StGB) ist von 681 im Jahr 2016 auf 733 im Jahr 2017 angestiegen. Die Zahl der Anzeigen wegen Groomings (§ 208a StGB) ist von 80 Anzeigen auf 106 Anzeigen im Jahr 2017 angestiegen. Die Zahl der Hinweise, die in der Meldestelle Kinderpornografie und Kindersextourismus im BK eingegangen sind, war ansteigend (2016: 1.530 Hinweise, davon 347 mit Österreichbezug; 2017: 1.698 Hinweise, davon 499 mit Österreichbezug). Die Mitarbeiter der Meldestelle für Kinderpornografie und Kindersextourismus im BK führten 2017 zahlreiche erfolgreiche Amtshandlungen, bei denen sexuelle Missbräuche an Kindern geklärt und umfangreiches Beweismaterial sichergestellt werden konnte."

(Quelle: https://www.bmi.gv.at/508/files/SIB_2017/01_SIB_2017-Hauptteil_web.pdf S. 33, abgerufen am 18.7.2019).

Der Lagebericht Cybercrime 2017 des Bundeskriminalamts (BKA) beginnt mit einer Darstellung der Organisationsstruktur zur Cybercrime-Bekämpfung. Im Jahr 2011 wurde das Cybercrime-Competence-Center (C4) im Bundeskriminalamt eingerichtet, welches aus vier Referaten besteht:

1. Zentrale Aufgaben,
2. IT-Beweissicherung mit den Fachbereichen IT-Forensik und Mobile Forensics,
3. Ermittlungen mit dem Fachbereich Automatischer Datenabgleich (ADA) und Datenbanken,
4. Entwicklung und Innovation.

Zu den Cybercrime-Schwerpunkten 2017 gehörte vor allem Ransomware mit der Schadsoftware Petya/NotPetya und WannaCry, mit denen weltweit hunderttausende Computer infiziert wurden. Die für Ransomware eingerichtete SOKO Clavis verzeichnete deshalb in den Monaten Februar und März 2017 sprunghaft mehr Anzeigen. 2017 war auch das Jahr der Phishing E-Mails mit Links zu Schadsoftware oder Dateianhängen mit Malware, welche die Computerspeichersysteme verschlüsselt. Ende 2017 kamen neue Angriffsvektoren über die Remote Desktop Protokoll (RDP) Schnittstelle, die hauptsächlich für Benutzer-Unterstützung per Fernwartung durch einen zentralen IT-Helpdesk, Fernzugriff und Software-Wartung verwendet wird. Die Passwörter für den RDP-Zugriff werden von den Hackern durch „Brute Force Attacken" geknackt,

die darin bestehen, dass mittels automatisierten Ausprobierens einfache Passwörter so lange eingegeben werden, bis das richtige Passwort dabei ist. Damit haben dann Cyberkriminelle einen Zugang, mit dem das Opfer ausspioniert und dann erpresst wird. Ein Passwort bestehend ab 13 Zeichen, welches nicht im Wörterbuch/Telefonbuch/etc. steht und aus Zahlen, Groß-/Kleinbuchstaben und Sonderzeichen besteht, gilt 2017/18 noch als relativ sicher. Ab 2018 kommt bei den meisten Computersystemen die Zweifaktor-Authentifizierung, bei der zwei Faktoren den Zugang zum System ermöglichen, z.B. Passwort und Einmal-Code per Mobiltelefon.

Bei Distributed-Denial-of-Service (DDoS) Attacken werden ganze Computersysteme lahmgelegt. 2017 begann auch der Hype um die Kryptowährung Bitcoin, die auf der Blockchain-Technologie aufgebaut ist und für das „Mining" (Belohnung der Miner mit Bitcoins für komplexe Blockchain-Berechnungen) enorme Rechnerleistung und Stromkosten verschlingt. Dies brachte Kriminelle auf die Idee, Rechner illegal zu übernehmen und unbemerkt darauf zu „minen", was als Cryptojacking bezeichnet wird. 2017 setzte sich der Trend fort, dass Daten vermehrt auf verschlüsselten Datenträgern (z.B. Festplattenverschlüsselung bei Notebooks) und in der Cloud gespeichert werden.

Das Darknet (z.B. Cybercrime-as-a-service) stellte enorme Herausforderungen an die Ermittler, die dann per „Live-Forensik" ermittelten. Big Data mit beschlagnahmten Daten im dreistelligen Terabyte-Bereich erfordern effiziente Such- und Analyseverfahren (Massive Data Analysis) für die Cyberpolizisten. Elektronische Schließsysteme für Autos und Motorräder wurden von Kriminellen gehackt, was zu Diebstählen und Manipulationen auf der kriminellen Seite und zur Verstärkung der Fahrzeug-Forensik auf der kriminalpolizeilichen Seite führte.

Das autonome Fahren und Internet of Things (IoT) erfordern eine hohe IT-Security, damit nicht Kriminelle Schäden an Geräten anrichten können, die fatal für den Einzelnen aber auch für die gesamte Gesellschaft (terroristische Angriffe auf kritische Infrastrukturen (KRITIS) wie Kraftwerke, Wasserwerke, Fabriken mit giftigen Substanzen, Lebensmittelindustrie, etc.) werden können.

Daher spielen Prävention, Aufklärung und Bewusstseinsbildung für IT-Sicherheit eine immer wichtigere Rolle. Die Polizei bietet in Zukunft Upload-Plattformen an, auf denen Bürgerinnen und Bürger verdächtige Aktivitäten von z.B. Terroristen uploaden können, die dann zu schnelleren Ermittlungen führen und die Beweislage gegen Verdächtige festigen.

Angezeigt wurden laut Kriminalitätsbericht 2017:

- 363 Fälle von Hacking (§ 118a StGB)
- 1.186 Fälle von Datenbeschädigung (§ 126a StGB, hierunter werden Fälle von Ransomware gezählt)

- 105 Fälle von Störung der Funktionsfähigkeit eines Computersystems (§ 126b StGB)
- 189 Fälle von Missbrauch von Computerprogrammen oder Zugangsdaten (§ 126c)
- 1.056 Fälle von betrügerischem Datenverarbeitungsmissbrauch (§ 148a StGB)
- 231 Fälle von Datenfälschung (§ 225a StGB).
- 359 Fälle von Cybermobbing (§ 107c StGB neu seit 2016).

  (Quelle: https://bundeskriminalamt.at/306/files/Cybercrime_17_web.pdf, abgerufen am 21.8.2019)

Das Cybercrime Bundeslagebild des deutschen BKA 2017 weist in einer Zusammenfassung folgende Daten auf:

- 85.960 Fälle von Cybercrime im engeren Sinne (+ 4%)
- 251.617 Fälle mit dem Tatmittel Internet unter allen in der polizeilichen Kriminalitätsstatistik (PKS) erfassten Straftaten (4,4 % aller in der PKS erfassten Straftaten)
- 1.425 Fälle von Phishing mit Onlinebanking (-34,5%)
- 4.000 Euro/Fall durchschnittlicher Schaden beim Phishing im Onlinebanking (2016: 4000 Euro/Fall)
- 71,4 Mio. Euro Schaden im Bereich Computerbetrug (2016: 50,9 Mio Euro)
- Zunahme bei mobiler Malware (+54%)
- 17 Organisierte Kriminalität (OK)-Gruppierungen im Kriminalitätsbereich Cybercrime; 3% aller OK-Verfahren (2016: 22)

  (Quelle: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2017.html?nn=28110, abgerufen am 19.8.2019)

Der 2018 Internet Crime Report des FBI Internet Crime Complaint Centre (IC3) *(Quelle: https://pdf.ic3.gov/2018_IC3Report.pdf, abgerufen am 1.9.2019)* gibt einen Überblick über die Aktivitäten und Infrastrukturen des FBI zur Abwehr von Cybercrime in den USA und weltweit. Das IC3 ist eine Meldestelle, bei der im Jahr 2018 351.936 (2017: 301.580) Beschwerden eingingen und dies zu einem Gesamtschaden von 2,7 Milliarden (2017: 1,4 Milliarden) US-Dollar durch Cybercrime führte. Die häufigsten Betrugstrends im Jahr 2018 waren: Nichtzahlung/Nichtlieferung, Erpressung, Data Breach (Datenpanne, meist Diebstahl von personenbezogener Daten), BEC (Business E-Mail Compromise, BEC ist eine Betrugsart, die sich an Unternehmen richtet, die mit ausländischen Lieferanten zusammenarbeiten und/oder regelmäßig Zahlungen per Überweisung leisten), Vertrauens-/Romantikbetrug und EAC (E-Mail Account

Compromise, ähnlich wie BEC, ein Betrug, der sich an Einzelpersonen richtet), Betrug beim technischen Support und Gehaltsumleitung. Das FBI hat auch einige Infrastrukturen eingeführt, welche die Opfer unterstützen, den Schaden vergütet zu bekommen:

1. RAT (Recovery Asset Team) für die Unterstützung der Rückforderung von Geldern für Opfer von BEC-Programmen, insbesondere durch verbesserte Kommunikation mit Finanzinstituten; das RAT arbeitet innerhalb der
2. DFFKC (Domestic Financial Fraud Kill Chain), um Gelder, die von Opfern gestohlen wurden, zurückzugewinnen. Die DFFKC ist eine Partnerschaft zwischen Strafverfolgungs- und Finanzbehörden, die 2018 bei einem Schaden von 257 Millionen US-Dollar ca. 75% an die Opfer wieder zurückgeben konnte. Weiters wurde eine
3. VSIC-Stelle (Victim Specialists-Internet Crimes) eingerichtet. Die VSIC-Stelle nimmt Kontakt zu Opfern von Internetverbrechen auf, bieten Krisenintervention an, führen Bedarfsanalysen durch und weisen die Opfer gegebenenfalls auf Ressourcen und Empfehlungen hin. Damit soll sichergestellt werden, dass die Opfer rechtzeitig unterstützt und betreut werden, um eine weitere Verbrechenswiederholungen zu verhindern und den Wiederherstellungsprozess so schnell wie möglich einzuleiten.

Als Ergebnis des Vergleichs der Dokumente wurde herausgefunden, dass die österreichischen Fälle ähnlich verteilt sind, wie die in den Statistiken der oben genannten Quellen. Diese qualitative Analyse wurde von DI DDr. Walter Jaburek, gerichtlich beeideter Sachverständiger und Inhaber des Ingenieurbüros EDV-Concept GmbH, Wien im ersten Halbjahr 2019 durchgeführt.

So gab es vom zweiten Quartal 2017 bis zum ersten Quartal 2019 466 Fälle mit folgendem Lagebild:

Lagebild Gesamt	Anzahl Fälle	In Prozent
Erpressung	239	51,29%
Betrug	111	23,82%
Hacking	65	13,95%
Drohmails	14	3,00%
Viren	14	3,00%
Andere	23	4,94%
Gesamt	466	100,00%

Bei der Erpressung gab es 64 Fälle von Ransomware, gedroht wurde mit Abhören, Filmen über die PC-Kamera, Veröffentlichen der letztangesehenen Internetseiten, PC-Sperren und Mailsperren.

Ein Ticket vom 23.6.2017 mit Lagebild Ransomware lautete sinngemäß: „Letzte Woche wurde die Firma bereits das erste Mal von einem Verschlüsselungstrojaner attackiert. Leider war der externe Betreuer nicht in der Lage, dem Anrufer mitzuteilen, dass er die Festplatten ausstecken soll. Daher wünscht sich das Mitglied Unterstützung von uns. Am Montag wurde die Firma das zweite Mal attackiert. Auf allen 8 Festplatten sind die Daten verschlüsselt. Bei den verschlüsselten Dateiordern wurde die Zahlungsinformation und Netzwerkverbindung für die Kontaktaufnahme hinterlegt."

Ein Ticket vom 12.9.2018 mit Lagebild Erpressung per E-Mail hatte folgenden Inhalt: „Herr X hat ein Erpresser-E-Mail erhalten, in dem angedroht wird, dass er 300 US-Dollar auf ein Bitcoin-Konto einzahlen soll, da sonst von seiner eigenen E-Mail-Adresse office@xxxxxxxxxx.at an sämtliche Kontaktdaten, die er auf dem Rechner hat, ein Video gesendet wird, das pornografisches Material (von ihm selbst) enthält. Weiters wird erwähnt, dass nun eine RAT-Software (Remote Access Trojan) auf dem Rechner installiert sei."

Bei den Erpressungsfällen können mehr als die Hälfte der Tickets nicht durch das Sofortservice des Call-Centers gelöst werden, sondern erfordern den Einsatz eines „second levels", nämlich die Unterstützung durch die UBIT Cyber-Security-Unternehmen der CYS-Hotline.

Beim Lagebild Betrug gab es zwischen dem zweiten Quartal 2017 bis zum ersten Quartal 2019 111 Fälle:

Lagebild Betrug	Anzahl Fälle	In Prozent
Inkassobetrug	21	18,92%
BEC	24	21,62%
Phishing/Tech Support	41	36,94%
Überweisung	4	3,60%
Andere	21	18,92%
Gesamt	111	100,00%

Am 8.3.2019 wurde folgendes Ticket mit Lagebild „Fremdes E-Mail" aufgenommen: „Das Unternehmen X ist einem Internetbetrug zum Opfer gefallen. Eine Anzeige bei der Polizei wurde bereits eingebracht. Das Unternehmen

arbeitet mit einem chinesischen Lieferanten zusammen und hat von diesem eine Proforma-Rechnung mit einem schwedischen Konto erhalten, auf das das Unternehmen eingezahlt hat. Nach Rückfrage des chinesischen Lieferanten, wo das Geld ist, wurde bekannt, dass dieses schwedische Konto nichts mit der chinesischen Firma zu tun hatte, das Geld wurde bereits vom schwedischen Konto abgehoben."

Zum Lagebild „Tech Support" wurde am 28.11.2018 folgendes Ticket erfasst: „Herr X teilt mit, dass er soeben von der Firma Microsoft aus Kalifornien angerufen wurde. Laut denen wurde sein Computer mit einer Schadsoftware infiziert. Gleichzeitig wollte er von Herrn X wissen, wie viele Computer er hat bzw. dass er in der Kommandozeile etwas hineinschreiben soll. Herr X wollte noch kurz Rücksprache mit seinem Administrator halten. Der Herr von der angeblichen Microsoft Firma wollte ihm seinen Namen kein zweites Mal sagen und legte danach einfach auf. Es wurde nach keinem Lösegeld verlangt."

Bei der Bearbeitung der Betrugsfälle konnten beim Inkassobetrug ca. 75% sofort abgeschlossen werden, bei den anderen Betrugsarten ca. 40 – 60%.

Charakteristische andere Fälle im Zeitraum zwischen dem zweiten Quartal 2017 bis zum ersten Quartal 2019 waren:

Lagebild andere Fälle	Anzahl Fälle	In Prozent
Verleumdung, üble Nachrede	3	14,29%
Abhören	3	14,29%
Data Breach	2	9,52%
Technisch bedingter Datenverlust	1	4,76%
Gefälschte Homepage	3	14,29%
Geldwäsche	1	4,76%
Cold Calling	1	4,76%
Überhöhte Handy-rechnung	1	4,76%
Domain-Name-Steitigkeiten, Domain-Name-Verkauf	2	9,52%
Spam	4	19,05%
Gesamt	21	100,00%

Folgendes Beispiel vom 22.2.2019 entspricht dem Lagebild der „üblen Nachrede“: „Nach Kündigung eines Mitarbeiters wird über den Betrieb negativ auf sozialen Netzwerken gepostet. Frau X möchte wissen ob/wie sie dagegen vorgehen kann.“
Ein Beispiel für ein Ticket für das Lagebild „Hacking“ wurde am 22.10.2018 bearbeitet: „Es wurde von einer externen E-MailAresse eine E-Mail an die Firma, mit dem Text auf Englisch gesendet: „Guten Tag mein Opfer, ich weiß Ihre Passwörter“. In der Firma gibt es keinen IT-Betreuer, an den sich die Chefin wenden kann. Sie ersucht um einen Rückruf eines IT-Security-Experten, der checken soll, ob dieses E-Mail ernst zu nehmen ist.“
Am 24.9.2018 wurde ein Ticket zum Lagebild: „Stalking“ an eine IT-Security-Firma der CYS-Hotline weitergeleitet: „Herr X bekommt immer Anrufe, und es meldet sich dann niemand. Er möchte wissen woher die Leute seine Telefonnummer haben und was er dagegen machen kann.“
Zum Lagebild: „Viren, Spyware“ wurde am 21.7.2018 folgendes Ticket bearbeitet: „Frau X kam über Google zu www.itplatz.net. Hier kam ein Popup von Microsoft: „Es ist ein Trojaner am PC und betrifft alle Geräte“. Der IT-Betreuer der Firma konnte keine Spyware-Software finden und hat ihr geraten, die beiden PCs neu zu installieren, was auch durchgeführt wurde. Frau X möchte derzeit noch keine Beratung von der IT-Security Firma, sondern wird sich mit ihrem externen Betreuer nochmals beraten, ob dieser noch Hilfestellung benötigt. Wenn nötig wird sich Frau X nochmals melden.“

Kooperation mit staatlichen Stellen und Organisationen/Vereinen

Die WKO Cyber-Security-Hotline kooperiert mit dem Bundesministerium für Inneres (BMI) und dem Bundeskriminalamt (BKA). Als Kontakt- und Koordinationsstelle fungiert die WKÖ (Servicemanagement und IKT, Mag. Christian Dosek). 2017 wurde eine Machbarkeitsstudie für ein KMU-CERT (Computer Emergency Response Team) in Auftrag gegeben, welche über das BMI-Projekt „Gemeinsam sicher für die Wirtschaft“ abgewickelt wurde. Die Studie wurde 2018 fertiggestellt und kommt zum Schluss, dass

- der Bedarf für ein KMU-CERT gegeben ist (Umfrageergebnis unter 400 Unternehmen),
- IT-Security-Dienstleister damit einen Zugriff zu CERT-Netzwerken haben,
- die WKO Cyber-Security-Hotline vom KMU-CERT profitiert und
- ein Kernteam aus vier bis sechs Personen den Start eines KMU-CERTs realisieren könnten.

Mit dem Bundeskriminalamt (BKA) wurde vereinbart, dass bei Anzeigen von Cybercrime-Vorfällen in Unternehmen, die bei der örtlichen Polizei eingebracht werden müssen, auf die WKO Cyber-Security-Hotline hingewiesen wird.
Bereits zur Startphase der Cyber-Security-Hotline wurde Kontakt mit Dr. Wolfgang Schwabl, Co-Vorsitzender der „Cyber Sicherheit Plattform“ (CSP, https://www.bka.gv.at/cyber-sicherheit-plattform), Bundeskanzleramt, aufgenommen, damit zügig eine informelle Abstimmung mit den nationalen, europäischen und internationalen IT-Security-Organisationen und -Unternehmen hergestellt wird.
Für das „Kuratorium Sicheres Österreich (KSÖ)“ ist Cyber-Security ein Themenschwerpunkt. Daher wurden auch seitens der KSÖ Landesgruppe Steiermark Cybersecurity-Veranstaltungen in Zusammenarbeit mit der WKO Cyber-Security-Hotline durchgeführt. Am 29.5.2017 fand im Europasaal der WKO Steiermark die Steirische KSÖ Konferenz „Sicherheit im digitalen Zeitalter“ statt, bei der die WKO Cyber-Security-Hotline erstmals öffentlich angekündigt wurde. Am 22.6.2018 fand die KSÖ Sicherheitskonferenz in Bad Radkersburg statt. Am 14.3.2019 war das KSÖ Partner für die Veranstaltung “Rethink Cybersecurity” in der WKÖ.
Auch mit CERT.at und ACOnet-CERT wurde Kontakt aufgenommen. Mit CERT.at wurde vereinbart, dass nach Abklärung rechtlicher und organisatorischer Belange Indicators of Compromise (IoC)-Meldungen der WKO Cyber-Security-Hotline an CERT.at und dann folglich CERT.at-Warnungen an die Unternehmen im Zuge von WKO-Aussendungen übermittelt werden.

Forschungsprojekte

Das wissenschaftliche Projekt: „Cybersecurity in Styria“ wurde im Jahr 2018 beim Land Steiermark erfolgreich eingereicht und wird bis 31.12.2019 fertig gestellt. Die Projektkoordination obliegt dem Institut für Philosophie (Politische Philosophie) der Karl Franzens Universität Graz. Projektpartner sind: Zentrum für Sozialforschung der Karl Franzens Universität Graz, Institut für Rechtswissenschaftliche Grundlagen (Fachbereich Recht und IT) der Karl Franzens Universität Graz, evolaris Next Level GmbH und Wirtschaftskammer Steiermark. Ziele dieser wissenschaftlichen Arbeit sind:

1. ein vertieftes Verständnis von Cybersecurity in Unternehmen zu erhalten,
2. Klärung der sozialen und ethischen Herausforderungen, um eine umfassende Sicherheit der NutzerInnen von IKT zu gewährleisten,
3. einen Kriterienkatalog zu erstellen,
4. Empfehlungen auszuarbeiten

Zukunft

Folgende Projekte für die Weiterentwicklung der Cyber-Security-Hotline sind definiert:

1. Strategie und Mission Statement mit WKÖ, WKO Landeskammern, Sprechern und UBIT-ExpertInnen der IT Security ExpertsGroup entwickeln,
2. Erstellung des Arbeitsprogramms für die Jahre 2020 und 2021,
3. Erstellung Detailanalysen und Lessons Learned,
4. Kommunikation verbessern (Call Center, Projektleitung, Sprecher, Landeskammer-Verantwortliche, Experten, Umfeld),
5. CYS-Hotline Konferenz 2 x pro Jahr,
6. virtueller Cyber-Security Summit mit ExpertInnen,
7. Cyber-Security Newsletter,
8. KMU-CERT,
9. Änderung des Workflows von geografischer Nähe zu IT-Security-Firmen-ExpertInnenprofile,
10. Cyber-Security Versicherungen,
11. Sicherheits-App,
12. Internet Fernsehen erweitern: Cysec.tv
13. Kooperationen mit Forschungspartnern und Cyber-Security-Unternehmen,
14. Online-Realtime Cyber-Security-Landkarte Österreich mit einem Cyber-Security-Barometer als Frühwarnsystem für Unternehmen,
15. Cybercrime-Anzeigeleitfaden sowohl für Polizei als auch Unternehmen.

Besuchen Sie im Web folgende Seiten:

Cys.at

Cysec.tv

www.it-safe.at

www.gemeinsamsicher.at