kaspersky

News zur Cybersicherheits-Politik

Juli / 2020

Auf ein Wort!

Erinnern Sie sich, was Sie am 10. März dieses Jahres gemacht haben? Ich erinnere mich sehr genau! Ich befand mich auf meiner letzten Geschäftsreise vor dem Corona-Lockdown. An diesem Tag hatte ich eine völlig andere Sicht auf die Welt und hätte viele Fragen anders beantwortet als heute. Ich hatte keine Vorstellungen von den einschneidenden, notwendigen und zugleich vernünftigen Maßnahmen zur Bekämpfung der Corona-Pandemie. Ich hatte eine andere Einstellung dazu, was im Geschäftsleben sinnvoll ist und was nicht. Zum Beispiel, ob es eine gute Idee ist, eine bis dahin unbekannte Person im geschäftlichen Umfeld zum ersten Mal per Videokonferenz zu treffen? Oder, ob Onlineunterricht an Schulen sinnvoll möglich ist? Wir haben sehr herausfordernde Monate hinter uns, aber auch vor uns. Wir müssen uns weiter verändern und lernen. Wir müssen die Digitalisierung mutig vorantreiben. Das ist eine meiner Kernerkenntnisse aus der Corona-Krise, neben der Tatsache, achtsam zu sein. Dies gilt insbesondere in Fragen der Cybersicherheit. Mit der ersten Ausgabe dieses Newsletters möchten wir hierzu beitragen. Es würde mich sehr freuen, wenn Sie beim Lesen den einen oder anderen Impuls aufnehmen würden und wir darüber ins Gespräch kommen könnten. Ich freue mich auf Ihr Feedback!

Jochen Michels
Head of Public Affairs Europe, Kaspersky

Globale Transparenz-Initiative: Cyber-Capacity-Building-Programm gestartet

Kaspersky entwickelt seine Globale Transparenzinitiative (GTI) weiter. Die bereits ergriffenen Maßnahmen – wie die Verlagerung europäischer Nutzerdaten nach Zürich, die Eröffnung von Transparenzzentren in mehreren Ländern zur Überprüfung von Quellcodes, die Auditierung der zuverlässigen und sicheren Geschäftsprozesse durch das unabhängige SOC 2-Audit und die ISO27001-Zertifizierung – zeigen, dass die GTI eine einzigartige Initiative zur Steigerung von Transparenz und Vertrauen in der digitalen Welt ist. Im Mai hat Kaspersky weitere Maßnahmen ergriffen. Hierzu zählen unter anderem:

Cyber Capacity Building Programm

Dieses spezielle Schulungsprogramm vermittelt Unternehmen, Regierungsorganisationen und akademischen Einrichtungen Kenntnisse und Fertigkeiten, um die Sicherheit digitaler Produkte und Lösungen eigenständig evaluieren zu können. Schulungsteilnehmer erwerben umfassende Fähigkeiten zur Bewertung der Cyber-Resilienz der von ihnen eingesetzten IT Systeme. Das ist besonders dann wichtig, wenn Unternehmen Bestandteil globaler Lieferketten oder kritischer Infrastrukturen sind. Fallen Komponenten der IT-Infrastruktur aus, kann die öffentliche Sicherheit beeinträchtigt werden und wirtschaftlicher und sozialer Schaden entstehen. Vor diesem Hintergrund ist die Fähigkeit gefragt, die Sicherheit und Integrität dieser Elemente zu bewerten und einen verlässlichen Betrieb zu gewährleisten.

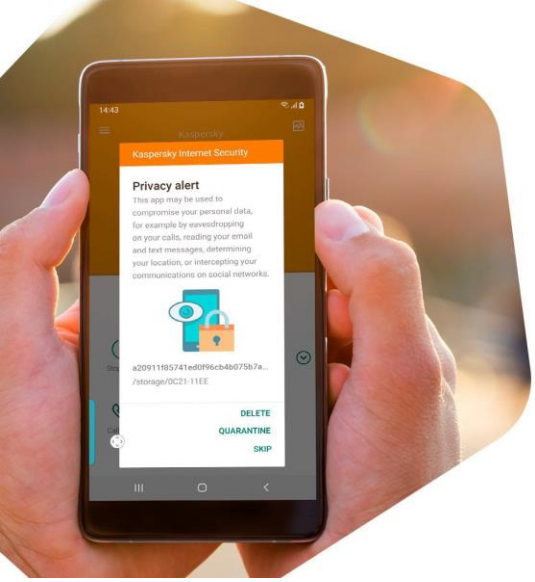
Das Cyber-Capacity-Building-Programm setzt genau an diesem Punkt an. Es ist online und offline in englischer Sprache verfügbar und wird kostenlos zur Verfügung gestellt. Die Schulung bietet eine Einführung in die Evaluierung von Produktsicherheit, in die Bedrohungsanalyse, die Überprüfung von Quellcode und in das Schwachstellenmanagement. Weitere Informationen erhalten Sie hier.

Virtueller Zugang zu den Transparenzzentren

Die Corona-Pandemie hat Kontakt- und Reiseverbote mit sich gebracht. Deswegen haben wir den bislang rein physischen Zugang zu den Transparenzzentren überdacht. Künftig bieten wir die so genannte „Blue Piste"-Evaluierung online an. Fordern Sie hier eine Tour an.

Verantwortungsvolle Offenlegung von Schwachstellen

Wir arbeiten sehr vertrauensvoll mit der Cybersicherheits-Community zusammen, um die Sicherheit unserer Produkte kontinuierlich zu verbessern. Hierfür haben wir ethische Grundsätze entwickelt, die auf unseren Erfahrungen und den von FIRST zur Verfügung gestellten Richtlinien beruhen. Sie zielen darauf ab, Transparenz sowie Effizienz im Umgang mit Schwachstellen zu erhöhen und Schäden und Risiken für Nutzer zu minimieren: Weitere Infos.



Stalkerware – eine wachsende Cyber-Bedrohung

Stalkerware: Hinter diesen Begriffen verbirgt sich ein noch wenig bekanntes, aber sehr ernsthaftes und wachsendes Problem. Kurz gesagt handelt es sich dabei um Spy- oder Tracking-Software, die es ermöglicht, das Privatleben einer Person zu verfolgen, indem sie auf ihre persönlichen Daten zugreift: Kontakte, Anrufprotokolle, Fotos, Videos, SMS-Nachrichten, Standortinformationen. Stalkerware kann „legal" erworben und von jeder Person, die physischen Zugang zu einem Endgerät hat, installiert werden. Nicht legal ist die Nutzung von Stalkerware, wenn die Software ohne Einwilligung des Benutzers installiert wurde und sich die Software auf dem Gerät „versteckt", das Opfer also ohne sein Wissen ausspioniert. Auch wenn die Überwachung bzw. das Stalking online erfolgt – die Folgen für die Opfer sind oft weitreichend und schwerwiegend. Zudem geht Cyber-Stalking häufig mit häuslicher Gewalt einher.

Als Antwort auf den zunehmenden Einsatz solch schädlicher Software haben *Kaspersky* und neun Partnerorganisationen aus verschiedenen Ländern – *Avira, Electronic Frontier Foundation, European Network for Working with Perpetrators of Domestic Violence (WWP EN), DATA CyberDefense, Malwarebytes, Nationales Netzwerk gegen häusliche Gewalt (NNEDV), NortonLifeLock, Operation: Safe Escape und WEISSER RING* – im November 2019 die „Coalition against Stalkerware" gegründet.

www.stopstalkerware.org

COALITION AGAINST STALKERWARE

Die Gründungsmitglieder haben in einem ersten Schritt eine Definition für Stalkerware erarbeitet und gemeinsame Kriterien definiert, um Stalkerware zu erkennen und Nutzer zu warnen.

Zu den Zielen der Koalition gehören:

- Verbesserung der Erkennung und Eindämmung von Stalkerware,
- Erhöhung der technischen Fähigkeiten und Fertigkeiten von Opfern und Beratungs-Organisationen, und
- eine umfassende Sensibilisierung und Aufklärung.

+32%

Anstieg von Stalkerware im Jahr 2019, die von Kaspersky-Lösungen erkannt wurden, wobei sich die Zahl der Angriffe in der zweiten Jahreshälfte verdoppelt

Globale Trends

Russland, Brasilien, Indien und die Vereinigten Staaten sind die am stärksten betroffenen Länder der Welt. In Europa sind es Deutschland, Italien und Frankreich.

70 %

der Frauen, die Opfer von Cyber-Stalking waren, haben laut einer Studie des Europäischen Instituts für Gleichstellungsfragen auch mindestens eine Form körperlicher oder/und sexueller Gewalt von einem Beziehungspartner erlebt.

Angesichts der hohen gesellschaftlichen Bedeutung, des starken Wachstums des Missbrauches von Stalkerware und des hohen Gewaltpotenziales – etwa körperliche Gewalt gegen das Opfer nach Entdeckung und Entfernung der Software – strebt die Koalition eine noch breitere Zusammenarbeit an. Elf neue Mitglieder, viele davon aus der Europäischen Union, traten der Koalition im Mai 2020 bei.

« „Laut der vom Center Hubertine Auclert in Frankreich durchgeführten Studie[1] über Cyberkriminalität in Partnerbeziehungen haben 21% der Opfer den Einsatz von Stalkerware durch ihren Partner erlebt, während 69% der Opfer das Gefühl hatten, dass ihre persönlichen Daten auf ihrem Smartphone von ihrem Partner versteckt abgerufen wurden. Insgesamt ist Stalkerware eine schwerwiegende Gefahren- und Stressquelle für die Opfer. Die Koalition ist eine gute Gelegenheit, das Fachwissen des IT-Sicherheitssektors und der auf Gewalt gegen Frauen spezialisierten NGOs zusammenzubringen. Diese Zusammenarbeit auf internationaler Ebene wird fruchtbar sein, um gemeinsam die besten Lösungen für den Schutz der Opfer zu finden. »

Clémence Pajot, Director of the Centre Hubertine Auclert

Aufgabe des Zentrums ist die Förderung von Gleichstellung und die Bekämpfung von Gewalt gegen Frauen in der Region Paris.

1 https://www.centre-hubertine-auclert.fr/outil/rapport-cyberviolences-conjugales-2018

COVID-19-Pandemie: Auswirkungen auf die Cybersicherheit von Organisationen und Einzelpersonen?

Drei Fragen an Marco Preuss, Leiter des EU-Teams des Global Research & Analysis Team (GReAT) von Kaspersky.

Hat die Zahl der Cyber-Angriffe während des Lockdowns zugenommen?
Der Lockdown wurde schnell zu einem Wettlauf um hohe Angriffszahlen, welche meist ohne konkrete Belege veröffentlicht wurden, um Nachrichten zu generieren. Im Mai stellte beispielsweise ein Verleger eine „Zunahme der Angriffe von mehr als 30.000%“ fest. Es ist jedoch fraglich, woher diese menschlichen Kapazitäten für eine derartige Zunahme kommen sollten? Sind Angreifer aktiver und schneller geworden? Nein, die Möglichkeiten für Computerangriffe haben sich nicht vervielfacht. Auch die Motivation der Kriminellen ist weitgehend gleich geblieben. Unsere Daten zeigen, dass die Erkennungszahlen von schädlichen Programmen im Zeitraum Januar bis Mai 2020 im Vergleich zum gleichen Zeitraum 2019 weltweit nicht zugenommen haben. Jedoch wurde die Aufmerksamkeit rund um das Thema COVID-19 genutzt, um entsprechende Cyber-Angriffe zu fahren: zwischen Januar und März haben wir einen 43%igen Anstieg dieses Themas als Aufhänger bei Phishing-Versuchen festgestellt. Cyberkriminelle haben auch mit Schadsoftware versehende Videokonferenzeinladungen, falsche Zertifikate, Benachrichtigungen über fehlgeschlagene Paketzustellungen oder sogar falsche Entlassungen verschickt. Wir haben zwischen Januar und April 2020 zudem einen 25%igen Anstieg bei der Erkennung von internetbasierten Bedrohungen erkannt. Man könnte versucht sein, dieses Phänomen mit einem Anstieg der Angriffszahlen zu erklären, die diese Vektoren ausnutzen. Gleichzeitig können erhöhte Zahlen aber auch einfach eine Folge der erhöhten digitalen Nutzung während des „Lockdowns“ gewesen sein und müssen deshalb nicht auf einen Anstieg an Angriffen oder eine höhere Erfolgswahrscheinlichkeit hindeuten.

Kostenloser Schutz für mehr als 1.500 Gesundheitsorganisationen während der Pandemie

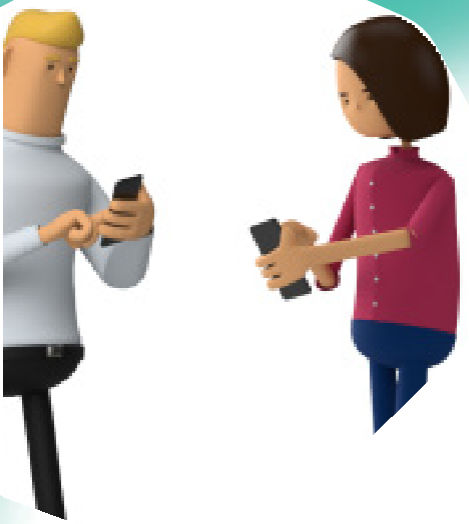
Aus Solidarität im Kampf gegen COVID-19 stellt Kaspersky öffentlichen und privaten Gesundheitseinrichtungen, für sechs Monate Ihre Software kostenfrei zur Verfügung. Mehr als 1.500 Krankenhäuser und Gesundheitsorganisationen weltweit haben dieses Angebot bislang genutzt.

Die Corona-Krise hat zu einem massiven Anstieg an Telearbeit geführt. Welche Lehren können wir aus dieser Zeit ziehen?

Die technischen Ressourcen für die Telearbeit (VPNs, Kollaborations- oder Videokonferenzplattformen, Laptops) mussten schnell zur Verfügung gestellt und vielleicht auch außerhalb der sonst üblichen Verfahren verteilt werden. In der Eile wurden Sicherheitsmaßnahmen möglicherweise vernachlässigt. Eine funktionierende, verfügbare und sichere IT ist für jede Organisation von wesentlicher Bedeutung. In einer solchen Krise ist sie mehr denn je Voraussetzung für den Geschäftsbetrieb. Manager müssen daher ihre Organisation mit angemessenen Sicherheitsressourcen ausstatten – bevor es zu einer Krise kommt. Denn in einer Ausnahmesituation wie zu Beginn der Corona-Pandemie muss man den Geschäftsbetrieb möglichst unterbrechungsfrei, sicher und in guter Qualität aufrechterhalten können. Die zweite Lektion ist, dass moderne digitale Arbeitsmittel für die Zusammenarbeit gedacht sind und strukturiert verteilt werden sollten. Noch wichtiger ist allerdings, dass ihre sichere Nutzung bei der Telearbeit auf Basis des „Defence in Depth"-Paradigmas erfolgen sollte. Allzu oft beziehen sich Sicherheitslösungen noch immer auf einen begrenzten und kontrollierten Umkreis (das Unternehmen, sein Netzwerk und seine Räumlichkeiten), der vor dem „Rest" schützt. Es muss jedoch berücksichtigt werden, dass jede IT-Ressource (einschließlich Daten und Arbeitsstationen) individuell und überall exponiert werden kann und daher unabhängig zu schützen ist. Dies erfordert insbesondere die Fähigkeit, externe Arbeitsstationen unter sicheren Bedingungen zu warten. Es können viele Lehren daraus gezogen werden, aber ich möchte als letzten Punkt die Wachsamkeit nehmen: Verschiedene Lösungen, die unter dem Namen „Cloud" vermarktet werden, scheinen die Antwort auf alle digitalen Herausforderungen zu sein, die durch die aktuelle Krise aufgezeigt wurden. Sie müssen aber mindestens ebenso viele Sicherheitsanforderungen erfüllen wie ihre Vorgänger. Darüber hinaus bringen sie eine schwer einzudämmende Abhängigkeit von Dritten mit sich, die im Krisenfall zu einer großen Schwachstelle werden kann. Darüber hinaus bestehen Schwierigkeiten bei der Datenkontrolle. Der Einsatz solcher Lösungen kann auch zu einer weiteren Verringerung der unternehmenseigenen IT-Kapazitäten führen, die für die Bewältigung von Ausnahmesituationen unerlässlich sind.

Gab es aufgrund der nicht-steigenden Zahl an Cyberangriffen während der Pandemie Entwicklungen in diesem Bereich?

Bereits im Januar gab es gezielte Kampagnen mit Schadsoftware behafteten Nachrichten gegen Regierungsorganisationen in Asien und Europa. Das meiste Schadmaterial, welches wir in diesem Zusammenhang entdeckt haben, umfasste Statistiken über die Verbreitung des Corona Virus sowie Protokolle internationaler Treffen. Die von diesen Akteuren angewandten Methoden, um in Netzwerke einzudringen, haben sich jedoch während der Pandemie nicht geändert. Bei anderen Attacken wurden unter dem Deckmantel von Tools zur Infektionsverfolgung schädliche mobile Anwendungen freigeschaltet. Wir haben zudem festgestellt, dass Organisationen des Gesundheitssektors, einschließlich internationaler Organisationen, zu Beginn dieses Jahres besonders ins Visier gerieten. Letztere wurden wahrscheinlich angegriffen, um nachrichtendienstliche Erkenntnisse zum Gesundheitskrisenmanagement zu sammeln und so internationale politische Strategien antizipieren zu können. Angesichts der Tatsache, dass „Hacken" mittlerweile Bestandteil vieler nachrichtendienstlicher Methoden ist und das Corona Virus im Fokus des internationalen Interesses steht, war dies zu erwarten. Wir haben auch einige Fälle gezielter Ransom-Attacken identifiziert, bei denen bekannte Schwachstellen von VPN-Gateways ausgenutzt wurden. Es ist möglich, dass diese Geräte während der Pandemie besonders ins Visier genommen wurden, da die Angreifer ihre übereilte Exposition ausnutzen wollten und Opfer in einer Krisensituation wahrscheinlich eher Lösegeld zahlen würden. Schließlich haben wir auch einen signifikanten Anstieg (+80%) an Netzwerk-Denial of Service-Versuchen im ersten Quartal 2020 im Vergleich zum Vorjahresquartal beobachtet. Diese Versuche zielten hauptsächlich auf pädagogische und öffentliche Einrichtungen ab. Krisensituation bewegen Angreifer keinesfalls zu einem Waffenstillstand. Im Gegenteil: Jedes Ereignis, das Aufmerksamkeit erregt, wird von Cyberkriminellen ausgenutzt. Um Ungewissheit zu verringern und übermäßige Zwischenfälle zu vermeiden, sind die eigenen IT-Ressourcen permanent zu überwachen und zu schützen. Zudem sind Maßnahmen zur Aufrechterhaltung des Betriebs vorzubereiten, die die Nichtverfügbarkeit dieser Ressourcen berücksichtigen.



Sichere elektronische Abstimmungen als Grundlage für die E-Demokratie

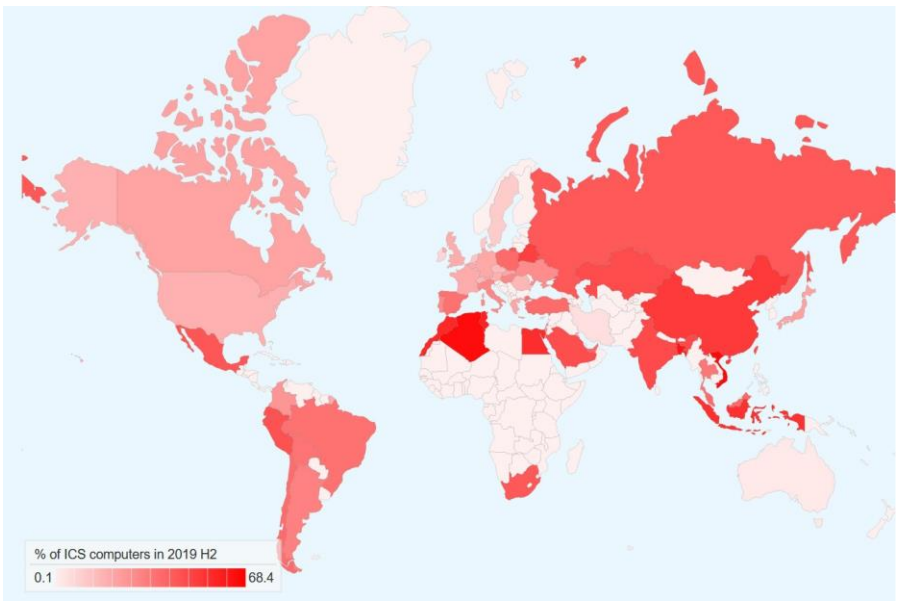
Online-Wahlen haben viele Vorteile: Sie sind kostengünstig, sie sparen dem Wähler und den Organisatoren Zeit und sie sind effizient. Doch am Anfang eines solchen Prozesses steht zunächst eine Investition, denn die Anforderungen an die Sicherheit und Zuverlässigkeit von Online-Wahlen sind erheblich. Auch deswegen gab es in der Vergangenheit oft einige Hindernisse, wenn es um die Einführung von Online-Wahlen ging.

Die aktuelle Corona-Pandemie hat hier einen neuen Impuls für digitale Lösungen gebracht – auf vielen Ebenen. Von jetzt auf gleich gab es den Bedarf, schnell und effizient elektronische Abstimmungssysteme zu implementieren. Auch wenn die Abgeordneten nicht im Parlament, sondern in ihren Wahlkreisen waren, standen Abstimmungen auf der Agenda. Das Gleiche gilt und galt für Unternehmen, Verbände, Gewerkschaften und politische Parteien, bei denen Abstimmungsprozesse und Wahlen auf der Agenda stehen und standen, die idealerweise digital möglich sein sollen. Dieser Trend wird sich künftig weiter verstärken. Und die Einstellung von Gesellschaft, Politik und Wählern zu elektronischen Abstimmungen und Wahlen wird sich vermutlich positiv verändern.

Kaspersky trägt zu diesem Übergang mit seiner neuen, auf Blockchain-Technologie basierenden Plattform für elektronische Abstimmungen Polys bei. Polys ist ein umfassendes, sicheres Online-Abstimmungssystem. Es basiert auf einer über mehrere Knotenpunkte dezentralisierten Architektur. Je nach Anforderung des Organisators kann diese bei einem vertrauenswürdigen Dritten in der Cloud oder vor Ort gespeichert werden. Ein weiterer Bestandteil der Lösung sind sichere physische Wahlmaschinen und Wahlurnen, die an die Blockchain angeschlossen sind. Auf diese Weise wird die Integrität und Unverletzlichkeit elektronischer Abstimmungen rechtskonform und sicher gewährleistet.

Kritische Industriesysteme: fast doppelt so viele Schwachstellen innerhalb eines Jahres

Neue Untersuchungen des ICS CERT von Kaspersky zur Bedrohung industrieller Kontrollsysteme (ICS) identifizierten 103 neue Schwachstellen im Jahr 2019, die von Cyberattacken ausgenutzt werden könnten. Das sind fast doppelt so viele wie 2018. Von diesen waren 33 am Ende des ersten Quartals 2020 noch immer nicht von den Herstellern behoben. Dabei ist die Bedrohung nicht zu unterschätzen: 2019 wurden auf fast jedem zweiten ICS-System (46,4%), das am Kaspersky-Sicherheitsnetzwerk angeschlossen ist, schädliche Objekte blockiert, unabhängig davon, ob es sich dabei um Automatisierungssoftware, industrielle Steuerungssysteme oder das Internet der Dinge (IoT) handelte. Interessant ist, dass generische Bedrohungen auch auf spezialisierte industrielle Systeme abzielen: Ransomware (Wannacry – wieder einmal, GandCrab, etc.), die potenziell verheerendste Bedrohung, wurde auf 1% der von Kaspersky geschützten ICS-Systeme blockiert, insbesondere in Südostasien und Nordeuropa.



Der Energiesektor gehört weltweit zu den am stärksten betroffenen Sektoren: 36,6% der ICS-Systeme im Strom- und Energiesektor und 36,3% im Öl- und Gassektor waren Ziel eines Angriffs. Andere kritische Infrastrukturen und wesentliche Dienstleistungen – wie Wasseraufbereitung, Gesundheit und Lebensmittelverarbeitung – stehen bei der Erkennung von Schwachstellen ganz oben auf der Liste. Diese leider nicht sehr überraschenden Trends unterstreichen die Bedeutung regelmäßiger Sicherheitsaudits und einer aktiven Überwachung zum Schutz vor traditionellen Cyberkriminellen und APT-Gruppen.

Weitere Informationen: https://ics-cert.kaspersky.com/

Erster Kaspersky WebCast zur EU-Cybersicherheits-Politik mit mehr als 100 Teilnehmern und hochrangigen Referenten

Technologie, die auf den Menschen ausgerichtet ist: Warum eine angemessene Cybersicherheit entscheidend für die Digitalisierung ist“ – dieser Frage gingen aus unterschiedlichen Perspektiven namhafte Referenten der EU und der Mitgliedsstaaten beim ersten Kaspersky Webcast zu den Herausforderungen und Perspektiven der europäischen Cybersicherheitspolitik ein. Mit dem Thema und den Referenten schienen wir ins Schwarze getroffen haben: Mehr als 100 Teilnehmer nahmen an diesem interessanten Gedankenaustausch teil.

Ein Aspekt wurde schnell klar: Die Digitalisierung eröffnet große Chancen. Sie ist alternativlos. Aber die Verwundbarkeit gegenüber Cyber-Attacken hat in den vergangenen Jahren zugenommen. Mit dem Corona-bedingten Lockdown hat sich dieser Trend zudem beschleunigt. Dass viele Arbeitnehmer im Home-Office arbeiten und über das Internet auf das Firmennetz zugreifen, hat Cyberkriminellen neue Möglichkeiten eröffnet.

Diese Situation müsse gründlich reflektiert und langfristige Maßnahmen erarbeitet werden, forderte **Luisa Franchina**, Präsidentin des italienischen Verbands für kritische Infrastrukturen. Sie ermutigte die europäischen Interessenvertreter, Überlegungen zur Geschäftskontinuität künftig mehr Aufmerksamkeit zu schenken. Dabei sollten Vertrauen, Transparenz und gemeinsame Sicherheitsstandards die Grundlage für einen sichereren Cyberraum bilden.

Axel Voss, Mitglied des Europäischen Parlamentes, betonte, dass die Fragmentierung der Politik in der EU ein Nachteil sei. Die Union müsse in ihrer Gesetzgebung den digitalen Binnenmarkt fördern und stärken. Hierzu seien schnelle und effektive Maßnahmen erforderlich, um die anstehenden Herausforderungen der Cybersicherheit zu bewältigen und Cyber-Resilienz zu erreichen. Ein länderübergreifender Dialog unter Einbeziehung aller Interessengruppen sei der Schlüssel zur Gestaltung der Zukunft der Cybersicherheit: „Einheitliches Handeln ist der einzige Weg.“

Eric Bothorel, Abgeordneter der französischen Nationalversammlung, stellte auf den massiven digitalen Wandel ab, der die Gefährdung durch Cyberangriffe erhöht hat. Mehr als acht Millionen Franzosen würden derzeit Telearbeit leisten. Diese Mitarbeiter benötigten Unterstützung und Training sowie einen technisch sicheren Arbeitsplatz. „Wir müssen uns jetzt damit befassen und das Risiko heute bewältigen.“

CyberImmunity könnte die Lösung sein, erläuterte **Eugene Kaspersky**. Er machte klar, dass die derzeitigen Methoden des Risikomanagements nicht mehr ausreichen, um komplexe Infrastrukturen zu schützen. Deswegen müsse die Architektur aller Systeme in Richtung „Security-by-Design“ umgestaltet werden. Mit anderen Worten: „Sicherheit sollte zur DNA der Systeme werden: Nur so können sie wirklich unhackbar gemacht werden“.

Jakub Boratyński, amtierender Direktor des Direktorates H Digitale Gesellschaft, Vertrauen & Cybersicherheit bei der Europäischen Kommission, stellte fest, dass auf politischer Ebene die Herausforderung darin bestehe, die richtige Mischung von Anreizen zu finden, um die Cybersicherheitsrisiken auf einem akzeptablen Niveau zu halten. Künftige EU-Regulierungen sollten allen Akteuren – von den Staaten bis hin zu Sicherheitsanbietern und IT-Nutzern – in angemessener Weise Verantwortlichkeiten zuschreiben.

Wenn Sie daran interessiert sind, an weiteren Webinaren zu diesen Themen teilzunehmen, senden Sie uns bitte eine E-Mail an Kaspersky.EU-Policy@political-intelligence.com.

Wenn Sie diesen Newsletter bestellen (oder abbestellen) möchten, senden Sie eine E-Mail an: jochen.michels@kaspersky.com.

Kaspersky Europe

@Kaspersky_Gov @Kaspersky Kaspersky

kaspersky