DE

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

Von Januar 2019 bis April 2020

Ransomware

ENISA Threat Landscape

Überblick

Ransomware ist zu einer beliebten Waffe in den Händen böswilliger Akteure geworden, die täglich versuchen, Regierungen, Unternehmen und Einzelpersonen Schaden zuzufügen. In solchen Fällen kann das Opfer der Ransomware wirtschaftliche Verluste erleiden, indem es entweder das geforderte Lösegeld zahlt oder die Kosten für die Wiederherstellung des Verlusts zahlt, wenn es den Forderungen des Angreifers nicht entspricht. Bei einem Zwischenfall im Jahr 2019 in Baltimore, Maryland, kam es zu einem Lockout, und es wird erwartet, dass die Wiederherstellung 18,2 Millionen USD (ca. 15,4 Millionen EUR) kosten wird, obwohl die Stadt sich weigerte, das Lösegeld zu zahlen.[1] Mit der wachsenden Zahl von Zwischenfällen ist es offensichtlich, dass es nicht mehr maßgeblich ist, *ob* man ein Opfer wird, sondern eher, *wann*. Im Kampf der Länder gegen Ransomware müssen meist jedoch verschiedene Herausforderungen angegangen werden, z. B. die mangelnde Koordination und Zusammenarbeit zwischen Behörden und Ämtern sowie die fehlende Gesetzgebung, die Ransomware-Angriffe eindeutig unter Strafe stellt.

Obwohl es seit Anfang 2000 Cyber-Versicherungspolicen gibt[2], sind Ransomware-Angriffe einer der Hauptgründe für das in den letzten 5 Jahren gestiegene Interesse an dieser Art von Versicherung. In einigen der Vorfälle von 2019[7] wurden das Lösegeld oder die Kosten für die Wiederherstellung durch solche Verträge gedeckt. Wenn potenzielle Ransomware-Ziele als versichert bekannt sind, gehen die Angreifer jedoch leider davon aus, dass sie höchstwahrscheinlich bezahlt werden. Ein weiterer Nachteil für das Opfer ist, dass die Versicherer das Lösegeld im Voraus zahlen, um den Schaden zu mindern und den Ruf des Opfers aufrechtzuerhalten. Eine solche Compliance-Regelung durch die Zahlung von Lösegeld ermutigt jedoch die Hacker-Community und stellt weder die Wiederherstellung des Schadens noch die des Rufes des Opfers sicher.[3]

Erkenntnisse

€10,1_Milliarden wurden im Jahr 2019 schätzungsweise an Lösegeldern bezahlt

Die Höhe der gezahlten Lösegeldbeträge war um 3,3 Milliarden EUR höher als im Jahr 2018.

365 %_Zunahme der Entdeckungen in Unternehmen im Jahr 2019

Die Ransomware-Erkennung in Maschinen in Geschäftsumgebungen hat im Vergleich zum ersten Halbjahr 2018 zugenommen.[22]

66 %_der Gesundheitsorganisationen wurden angegriffen

Mehr als 66 % der Gesundheitsorganisationen erlebten einen Ransomware-Angriff im Jahr 2019.[23]

45 %_der angegriffenen Organisationen bezahlte das Lösegeld

Dies ist der Prozentsatz der Organisationen, die 2019 angegriffen wurden und das Lösegeld gezahlt haben; die Hälfte von ihnen hat jedoch ihre Daten nicht wiedererhalten.[37]

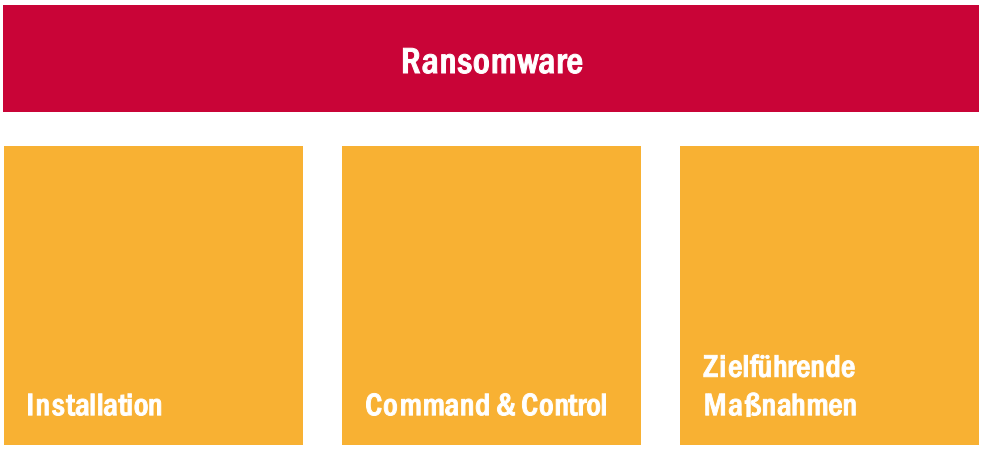
28 %_der Sicherheitsvorfälle wurden auf Malware zurückgeführt

Ransomware war nach Malware C2 die zweithäufigste Funktionalität und betraf ein Drittel (28 %) der Sicherheitsvorfälle.[32]

Kill chain

Schritt des Angriffs-Workflows

Umfang des Zwecks



Das Cyber Kill Chain® Framework wurde von Lockheed Martin entwickelt und basiert auf einem militärischen Konzept, das mit der Struktur eines Angriffs zusammenhängt. Um einen bestimmten Angriffsvektor zu untersuchen, verwenden Sie dieses Kill-Chain-Diagramm, um jeden Schritt des Prozesses sowie die vom Angreifer verwendeten Hilfsmittel, Techniken und Verfahren festzuhalten.

WEITERE INFORMATIONEN

Beschreibung

_Ransomware greift nach höheren Zielen

Die Ransomware-Angriffe im ersten und zweiten Quartal 2019 waren geringer als im gleichen Zeitraum der letzten drei Jahre. Diese Ransomware-Angriffe konzentrierten sich jedoch auf hochkarätige Ziele. Während des gesamten Jahres 2018 wurde die Bereitstellung von RAT (Remote Access Trojan), Downloadern und Backdoors festgestellt. In diesem Jahr blieb diese Malware jedoch im Leerlauf.[9,10] Es wird nun der Schluss gezogen, dass diese Software den Angreifern die Informationen zur Identifizierung gefährdeter High- Profilziele, die bereit sind, höhere Lösegeldbeträge zu zahlen, lieferte. Aus diesem Grund wurde Ransomware im Berichtsjahr auf andere Sektoren außerhalb des Gesundheitswesens ausgeweitet und richtete sich an Industrie- und Fertigungsunternehmen. Kürzlich wurde die Ransomware-Familie von LockerGoga verwendet, um Systeme zu beschädigen, die die physische Ausrüstung in Produktionsanlagen steuern.[11]

_Cyber-Versicherung beliebter

Cyber-Versicherungspolicen im Jahr 2019 stellten allein in den USA einen Markt von 8 Milliarden USD (ca. 6,7 Milliarden EUR) dar. Obwohl solche Produkte seit dem Jahr 2000 oder dem Millennium-Bug existieren, sind sie in den letzten Jahren für Regierungsorganisationen, Städte, Gesundheitsorganisationen und mehrere andere potenzielle Ransomware-Ziele mit hohem Risiko attraktiver geworden. Der SamSam-Angriff in Atlanta, Georgia, und der Vorfall in Lake City, Florida, wurden durch solche Richtlinien abgedeckt.[16] Mit steigenden Lösegeldforderungen werden Cyber-Versicherungspolicen für Organisationen und Unternehmen zunehmend notwendig. Der gesunde Menschenverstand legt jedoch nahe, dass die Opfer nach Möglichkeit vermeiden müssen, Forderungen nachzugeben. Wenn die Lösegeldforderungen erfüllt sind, wird nicht nur der Angreifer dazu verleitet, die Handlung zu wiederholen, sondern das Opfer kann sich auch nicht erholen, da sich der Angreifer in einigen Fällen nicht an die Abmachungen hält.

_Open Remote Desktop Protocol (RDP) ist ein hohes Risiko

Mehrere erfolgreiche Ransomware-Familien wie SamSam, BitPaymer und CrySiS zielen auf RDP-Server ab, um einen Angriff auszulösen.[20] Leider verwenden viele Unternehmen immer noch RDP anstelle des sichereren Virtual Private Network (VPN) für den Remotezugriff. Das Problem mit dem RDP besteht darin, dass es an Sicherheitslücken leidet, die ausgenutzt werden können, und dass der RDP-Dienst möglicherweise auf mit dem Internet verbundene Server angewiesen ist, auf die leicht zugegriffen werden kann. Es wurde berichtet, dass mehr als 800.000 Systeme mit RDP-Diensten nicht gepatcht und anfällig sind: Unter anderem Systeme im IP-Bereich des Microsoft Azure-Rechenzentrums.[51] Obwohl Microsoft der Öffentlichkeit versicherte, dass diese Systeme einem Drittanbieter gehören, tritt ein Problem hinsichtlich der Sicherheit von Cloud-Dienstanbietern auf.

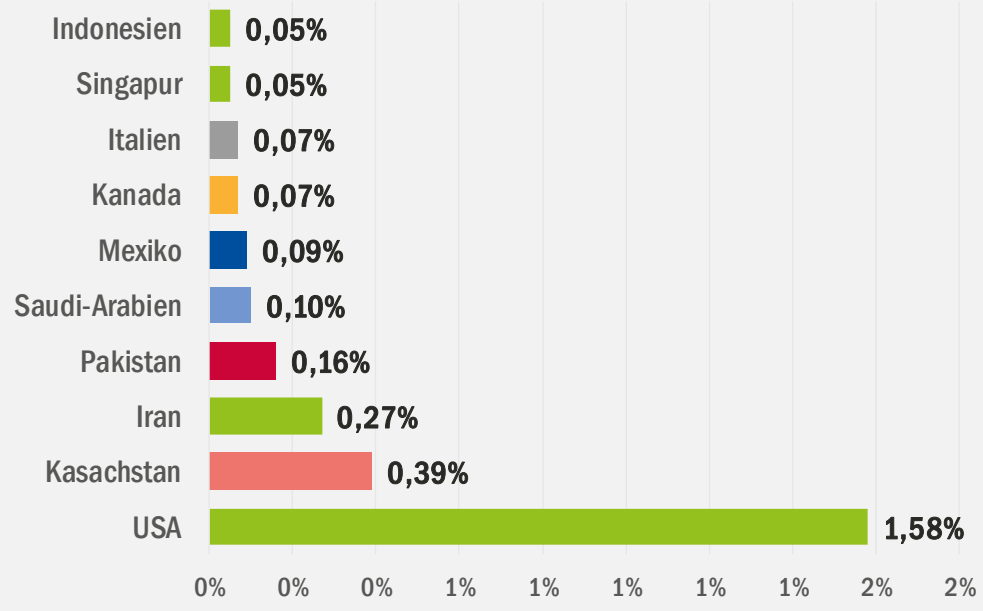


Abbildung 1: Top 10 Länder nach Anteil der Benutzer, die im 2. Quartal 2019 von mobilen Ransomware-Trojanern angegriffen wurden. Quelle: Kapersky[34]

Beschreibung

_ Die Beliebtesten

LOCKERGOGA_ wurde erstmals im Januar 2019 bei einem Angriff auf das französische Ingenieurbüro Altran Technologies gemeldet.[40] Die IT-Netzwerke und alle Anwendungen fielen aus, und die Geschäftstätigkeit des Unternehmens in mehreren Ländern war betroffen. LockerGoga wird vom PsExec-Tool gelöscht und ausgeführt, bei dem es sich um einen leichten Telnet-Ersatz handelt, der einige Sicherheitsüberprüfungen als halbgültige Software bestehen kann.[11] Nach der Installation werden die Benutzerkonten im Zielsystem geändert und das System wird zwangsweise abgemeldet. Darüber hinaus werden die Tool-Dateien selbst umbenannt und verschoben, sodass sie kaum mehr gefunden werden können. In späteren Versionen von LockerGoga ist die Sperrung so eng, dass die Opfer nicht einmal den Ransomware-Hinweis oder die Anweisungen zur Wiederherstellung sehen können, selbst wenn die Anforderungen erfüllt sind. Nur wenige Anti-Malware- und Antiviren-Produkte können Systeme gegen LockerGoga erkennen und verteidigen, und es gibt keinen bestimmten Entschlüsseler.[10] Abgesehen von Altran Technologies waren Hexor und Momentive von NorskHydro und zwei in den USA ansässigen Chemieunternehmen in 2019 durch LockerGoga betroffen.[41] Allein für den NorskHydro-Angriff wurden die Kosten des Schadens auf 50 Millionen USD (ca. 42 Millionen EUR) geschätzt.[21]

KATYUSHA_ ist ein Ransomware-Trojaner, der erstmals im Oktober 2018 verwendet wurde. Er verschlüsselt die Dateien des Opfers, löscht Schattenkopien und liefert Anhänge per E-Mail. Katyusha nutzt die Exploits EternalBlue und DoublePulsar, um sich zu verbreiten.[45] Leider sind noch keine Tools oder Entschlüsseler zur Verteidigung verfügbar.

JIGSAW_ verschlüsselt nicht nur die Dateien des Opfers, sondern löscht sie auch, wenn die Anforderungen nicht innerhalb der in der Regel angegebenen 24-Stunden-Frist erfüllt werden. Wenn das Opfer versucht, seinen Computer herunterzufahren, erhöht sich außerdem die Löschrate. Es ist kein Zufall, dass diese Ransomware nach einer Horrorfilmfigur benannt wurde.[45] Sicherheitsunternehmen veröffentlichen jedoch ständig Updates für einen effizienten Jigsaw-Entschlüsseler.[46]

PEWCRYPT_ wurde Anfang 2019 erstellt und im Gegensatz zu den meisten anderen Ransomware-Programmen besteht das einzige Ziel darin, die Benutzer zum Abonnieren des PewDiePie YouTuber-Kanals zu zwingen. PewDiePie war in einem Beliebtheitswettbewerb mit einem indischen Bollywood-Sender, T-Series, und seine Fans entschieden sich, PewCrypt zu verwenden, um die Gewinnchancen ihres Idols zu erhöhen. PewCrypt ist eine typische Ransomware, die durch Spam-E-Mails und böswillige Online-Werbung verbreitet wird. Sie wurde in der Programmiersprache Java erstellt. Im März 2019 veröffentlichte der Autor selbst ein Entschlüsselungswerkzeug.[47]

RYUK_ erschien erstmals im August 2018 und wurde als mit nordkoreanischen Hacking-Gruppen verbunden angesehen. Schon bald erwies sich, dass die Ryuk-Autoren dieselbe Gruppe waren, die dafür bekannt wurde, die Hermes-Ransomware zu verwenden und gleichzeitig ihren Code zu stehlen. Ryuks Hauptmerkmale sind die Verwendung militärischer Algorithmen und die gezielten Angriffe auf große Unternehmen. Darüber hinaus werden die meisten Opfer gebeten, das Lösegeld in Bitcoins zu zahlen.[45]

DHARMA_ ist ein Kryptovirus, das erstmals im Jahr 2016 aufgetreten ist, es werden jedoch weiterhin neue Versionen veröffentlicht. Dharma verschlüsselt nicht nur die Dateien des Opfers, sondern löscht auch alle Schattenkopien. Im Jahr 2019 wurde es durch kontaminierte Dateien mit beliebten, schädlichen oder legitimen Erweiterungen wie „.gif", „.AUF", „.USA", „.xwx", „.best" und „.heets" verbreitet. Im September 2019 veröffentlichte ein Sicherheitsforscher den Rakhnidecryptor[42], um Dharma-Opfern beim Entschlüsseln ihrer Dateien zu helfen.

GANDCRAB_ wurde im Januar 2018 zum ersten Mal verwendet und infizierte mehr als 50.000 Systeme in weniger als einem Monat. Damit wurde sie zu einer der beliebtesten Ransomwares von 2018.[43] Sie nutzt Microsoft Office-Makros, VBScript und PowerShell, um unentdeckt anzugreifen.[45] GandCrab ähnelt Cerber. Es basiert auf dem Ransomware-as-a-Service-Modell (RaaS) und ermöglicht Entwicklern und Kriminellen, Gewinne zu teilen. Einem Team von Europol, der rumänischen Polizei, der Generalstaatsanwaltschaft und Bitdefender gelang es, nach dem Hacken der GandCrab-Server ein Entschlüsselungswerkzeug zu produzieren[44]. Die Betreiber von GandCrab gaben ihren Rücktritt im zweiten Quartal 2019 bekannt, nachdem sie Lösegeldzahlungen in Höhe von mehr als 2 Milliarden USD gesammelt hatten. Die Sodinokibi-Ransomware, die in kleinen Kampagnen beobachtet wird, soll jedoch GandCrabs Nachfolger sein.[10]

Beschreibung

_ Die Beliebtesten

REVIL oder SODINOKIBI oder SODIN_ tauchten erstmals im Juni 2019 bei einem Webangriff auf das italienische WinRAR-Tool auf. Es wird auch vermutet, dass es an drei MSP-Angriffen und einem vierten gegen das amerikanische Unternehmen PerCSoft beteiligt ist, dessen Klientel hauptsächlich aus dem Gesundheitssektor stammt.[48] Sodinokibi scheint ein Produkt der bekannten Cyberspionagegruppe FruityArmor zu sein, die seit 2016 aktiv ist. Sodinokibi hat mehrere Länder weltweit betroffen. Taiwan hat bisher 17,56 % aller registrierten Sodinokibi-Angriffe erlitten, was es zu Sodinokibis Hauptzielland macht. In Europa sind Deutschland (8,05 %), Italien (5,12 %) und Spanien (4,88 %) die am stärksten betroffenen Länder. Sodinokibi wird von einem RaaS-Modell vertrieben und verschlüsselt die Dateien, die für einen Angriff pro System erforderlich sind. Die Angreifer binden einen „Skeleton Key" in ihren Code ein, mit dem sie Dateien unabhängig von der ursprünglichen Verschlüsselung aus der Ferne entschlüsseln können.[49] Wenn ein Computer jedoch über russische, armenische, syrische oder bestimmte andere Tastaturlayouts verfügt, kann Sodinokibi diese nicht verschlüsseln, eine Tatsache, die wahrscheinlich auf den Ursprung der Autoren hinweist.[50]

SAMSAM_ zielt zum fünften Mal in Folge weiterhin auf kritische Infrastrukturen weltweit ab. SamSam-Angriffe konzentrieren sich hauptsächlich auf Krankenhäuser, Gesundheitsunternehmen und Regierungsorganisationen, um eine schnelle Zahlung großer Lösegeldbeträge zu gewährleisten. Es nutzt Schwachstellen des Remote Desktop Protocol (RDP) aus. Bis heute hat die für den Vertrieb von SamSam verantwortliche Gruppe Lösegeldzahlungen in Höhe von mehr als 6 Millionen USD (ca. 5 Millionen EUR) gesammelt und die Opfer mehr als 30 Millionen USD (ca. 25,4 Millionen EUR) gekostet.[45] Ab 2018 beliefen sich allein bei einem Angriff auf die Stadt Atlanta die Schadens- und Wiederherstellungskosten auf 17 Millionen USD (ca. 14,4 Millionen EUR).[43]

"Die Komplexität der Bedrohungsfähigkeiten nahm 2019 zu, und viele Gegner nutzten Exploits, Diebstahl von Anmeldedaten und mehrstufige Angriffe."

In ETL 2020

Beschreibung

_ Zielbranchen

NATIONALSTAATEN SIND NOCH IMMER EINE ZIELSCHEIBE_ Im Jahr 2018 wurde Ransomware eingesetzt, um staatliche Organisationen als Geldquelle anzugreifen. Dieser Trend setzte sich 2019 fort, wobei Nationen oder Nationalgruppen ihre Identität mit denselben Instrumenten verschleierten, die von anderen Gruppen oder nationalstaatlichen Akteuren entwickelt wurden. Diese Manipulation von Instrumenten ermöglicht es der Herkunft des Angreifers, verborgen zu bleiben, und seinem Land, diplomatische Konsequenzen zu vermeiden, insbesondere wenn das Ziel eine Regierungs- oder staatliche Organisation ist.

Im Jahr 2019 fanden mehrere Angriffe gegen Regierungs- oder staatliche Organisationen statt, beispielsweise der, bei dem die kalifornische Stadt Lodi[4] aufgefordert wurde, Lösegeld in Höhe von 400.000 USD (ca. 340.000 EUR) zu zahlen, um aus einer Sperre der Telefonleitungen der Polizeibehörde, der Notrufnummer für öffentliche Arbeiten, den Nummern des Rathauses sowie der Zahlungsdaten und Finanzsysteme der Stadt entlassen zu werden. Die Stadt weigerte sich, der Forderung zu entsprechen und erholte sich durch Backups von dem Angriff. Das texanische Ministerium für Informationsressourcen meldete im August 2019 einen koordinierten Ransomware-Angriff auf 23 kleine Regierungsorganisationen.[5] Die Kosten für den Landkreis Texas wurden auf 3,25 Millionen USD (ca. 2,75 Millionen EUR) geschätzt. Baltimore erlitt einen RobbinHood-Angriff, der einen Schaden in Höhe von 18,2 Millionen USD (ca. 15,4 Millionen EUR) verursachte, während die Lake City in Florida einen Ryuk-Angriff erlebte, der einen Verlust von 460.000 USD (ca. 389.768 EUR) verursachte. Die Stadt New Bedford in Massachusetts wurde im Juli 2019 ebenfalls von einem Ransomware-Angriff heimgesucht (6) und forderte die Zahlung eines Lösegelds in Höhe von 5,3 Millionen USD (ca. 4,4 Millionen EUR). Die Stadt weigerte sich, das Lösegeld zu zahlen und gab stattdessen 1 Million USD aus, um sich von dem Angriff zu erholen.[7]

BILDUNGSEINRICHTUNGEN SIND MIT VON DER PARTEI_ Im Jahr 2019 beobachteten wir eine Verschiebung der Angriffe auf Bildungseinrichtungen. Laut einem Bericht der Sicherheitsfirma Emsisoft waren 1.051 Schulen und Hochschulen Opfer von 62 Ransomware-Vorfällen. Im Jahr 2018 waren es nur 11, bei denen Bildungseinrichtungen betroffen waren. Der Bericht erklärt, dass amerikanische Schulen nach den örtlichen Gemeinden die zweithäufigsten Opfer waren.[8]

DER GESUNDHEITSSEKTOR LEIDET WEITERHIN_ Organisationen des Gesundheitswesens waren in den vergangenen Jahren das bevorzugte Ziel von Ransomware-Angreifern, und dieser Trend setzte sich auch 2019 fort. Die kalifornischen Anbieter Wood Ranch Medical wurden im Sommer getroffen, und die elektronischen Patientenakten des Unternehmens (einschließlich der Backups) wurden aufgrund der Weigerung, das Lösegeld zu zahlen, vollständig zerstört. Der Vorfall zwang Wood Ranch Medical zu der Ankündigung, den Betrieb zum Jahresende einzustellen.[12] Im April 2019 ereignete sich genau die gleiche Abfolge von Ereignissen für einen anderen medizinischen Dienstleister, Michigan Brookside ENT und Hearing Centre[13], die ebenfalls gezwungen waren, zu schließen. Darüber hinaus wurden in Australien zwei Krankenhausgruppen angegriffen: Die GippslandHealth Alliance und die South West Alliance of Rural Health. Das Ergebnis war, dass Krankenhäuser in mehreren Städten, darunter Warrnambool, Colac, Geelong, Warragul, Sale und Bairnsdale, normale Patientenverfahren nicht erfüllen konnten, da ihre Systeme offline gingen, um die Exposition zu begrenzen.[14] In diesem Sektor ist der Datenverlust gleichermaßen schädlich wie der finanzielle Verlust. Beispielsweise sind die geschützten Gesundheitsinformationen von mehr als 300.000 Patienten infolge eines Ransomware-Angriffs im Juni 2019 gegen die Premier Family Medical-Gruppe in Utah durchgesickert.[15]

MSP FALLEN AUS_ Zahlreiche Branchen verlassen sich auf Managed Service Provider (MSP) und Cloud Service Provider (CSP), um vertrauliche Informationen zu hosten, die für ihren Betrieb unerlässlich sind. Sie verlassen sich auch auf sie, um die Integrität der Daten zu gewährleisten und den unbefugten Zugriff auf sie zu verhindern.[17] Die Ransomwares von GandCrab und Sodin zielen jedoch auf Schwachstellen in den MSPs ab, die ihre Infrastruktur und die von ihnen gehosteten Daten offenlegen, und ermöglichen schließlich, dass der Ransomware-Angriff sich auf die gesamte Kundschaft des MSP ausbreitet. Das Webroot2FA, ein gängiges MSP-Tool, bettet solche Schwachstellen ein und wurde 2019 in mehreren Fällen verwendet.[18] In diesem Jahr wurden mehrere MSPs innerhalb von nur drei Monaten angegriffen, darunter PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. und IT By Design.[19]

Angriffsvektoren

_ Wie

Eine neue Ransomware namens Sodinokibi nutzt die kürzlich angekündigte Sicherheitsanfälligkeit von Oracle WebLogic Server in CVE-2019-2725 aus, um Remotecodeausführungsfähigkeiten zu erlangen. Das Opfer ist infiziert, ohne dass Maßnahmen ergriffen wurden. Offizielle Patches wurden auch für die Oracle WebLogic Server-Versionen 10.3.6.0 und 12.1.3.0 veröffentlicht.[51] Derselbe Angriff nutzt die Sicherheitsanfälligkeit CVE-2018-8453 aus, um mehr (erhöhte) Benutzerrechte zu erlangen, Prozesse auf der schwarzen Liste zu beenden, Dateien auf der schwarzen Liste zu löschen und zu filtern.[48]

Eine weitere Sicherheitsanfälligkeit, CVE-2019-0708, wird auch zum Einschleusen von Ransomware verwendet. Es ermöglicht eine nicht autorisierte Verbindung über das Remote Desktop Protocol (RDP) von Microsoft. Im Mai 2019 veröffentlichte Microsoft Patches für die aktuellen Betriebssystemversionen (OS) sowie für die Versionen, die nicht mehr unterstützt werden.[51]

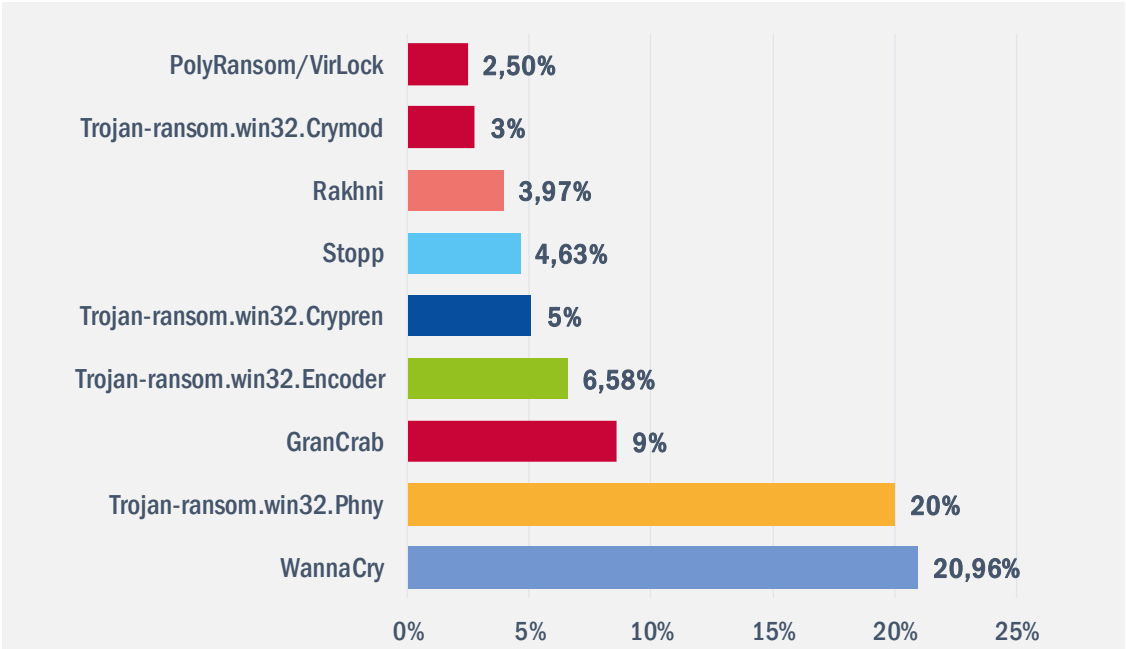


Abbildung 2: Die größten Ransomware-Angriffe in 2019. Quelle: Kapersky[39]

Vorfälle

- Der Baltimore County-Vorfall[1]
- Angriff auf Alabama Krankenhäuser[7]
- Lodi California City Vorfall[4]
- Texas (Texas Department of Information Resources) Vorfall[5]
- Lake City (Florida) Ryuk Angriff[7]
- New Belford (Massachusetts) Vorfall[6]
- Ransomware-Angriffe auf > 500 Schulen und Universitäten[8]
- Der Fall Wood Ranch Medical (California)[12]
- Michigan Brookside ENT und Hearing Centre Vorfall[13]
- Gippsland Health Alliance und der South West Alliance of Rural Health (Australien) Vorfall[14]
- Premier Family Medical Group (Utah) Vorfall[15]
- MSPs PM Consultants, CloudJumper, Datto, PercSoft, TSM Consulting Services Inc. und IT By Design Vorfälle[19]
- Microsoft Azure Datenzentrum Vorfall[51]
- Altran Technologies LockerGoga Angriff[40]
- Norsk Hydro LockerGoga Angriff[7]
- Hexion und die Momentive LockerGoga Angriffe[41]
- Albany IT Vorfall[60]
- Jackson County (Georgia) Vorfall[61]
- Riviera Beach (Florida) Vorfall[62]
- New Orleans Vorfall[63]
- Angriff auf den dänischen Hörgerätehersteller Demant[64]

Minderung

_ Vorgeschlagene Maßnahmen

- Sorgen Sie für zuverlässige Sicherungen, die der 3-2-1-Regel entsprechen (d. h. mindestens drei Kopien in zwei verschiedenen Formaten, wobei eine dieser Kopien außerhalb des Standorts bleibt).[5]
- Investieren Sie in eine Cyber-Versicherung, die Schäden durch Ransomware-Angriffe abdeckt.[21]
- Verwenden Sie Netzwerksegmentierung, Datenverschlüsselung, Zugriffskontrolle und Durchsetzung von Richtlinien, um eine minimale Datenexposition sicherzustellen.
- Verwenden Sie Methoden wie die Überwachung, um Infektionen schnell zu identifizieren.
- Überwachung des Status und des Zugriffs auf die verwendete öffentliche Infrastruktur.
- Erstellen Sie ein Security Operation Center (SOC) mit qualifiziertem Sicherheitspersonal in jeder Organisation oder Firma.
- Verwenden Sie geeignete und aktualisierte Instrumente zur Verhinderung von Ransomware.
- Definieren Sie genau und implementieren Sie einen Mindestsatz von Benutzerdatenzugriffsrechten, um die Auswirkungen von Angriffen zu minimieren (weniger Rechte, weniger Daten verschlüsselt).
- Implementieren Sie ein robustes Schwachstellen- und Patch-Management.
- Installieren Sie eine Inhaltsfilterung, um unerwünschte Anhänge, E-Mails mit schädlichem Inhalt, Spam und unerwünschten Netzwerkverkehr herauszufiltern.
- Installieren Sie den Endpunktschutz mithilfe von Antivirenprogrammen, blockieren Sie jedoch auch die Ausführung von Dateien (z. B. blockieren Sie die Ausführung im temporären Ordner).
- Verwenden Sie Richtlinien, um externe Geräte und die Barrierefreiheit zu steuern.
- Verwenden Sie die Whitelist, um zu verhindern, dass unbekannte ausführbare Dateien an Endpunkten ausgeführt werden.
- Investieren Sie in die Sensibilisierung der Benutzer für Ransomware, insbesondere im Hinblick auf ein sicheres Surfverhalten.

_Entschlüsseler

Erhebliche Fortschritte wurden durch EUROPOL erzielt, sowie 163 Partner mit dem „Kein Lösegeld mehr“-Projekt. Das Portal hat im Jahr 2019 28 Instrumente hinzugefügt und kann jetzt 140 verschiedene Arten von Ransomware-Infektionen entschlüsseln.[65] Eine Handvoll Ransomware-Entschlüsseler wurden entwickelt und viele andere aktualisiert. Im Folgenden sind Beispiele aufgeführt.

RANSOMWARE	ENTSCHLÜSSELER
Aurora[52], **Muhstik**[53], **Ryuk**[54]	Emsisoft
Rakhni, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Democry, TeslaCrypt, Chimera, Crysis, Jaff, Dharma, Cryakl, Yatron, FortuneCrypt,[55,56]	Kaspersky Lab
GandCrab[44]	Europol, Romanian Police und GPO, Bitfender
Jigsaw[46]	Avast
Mira[57]	F-Secure
Nemty[58]	Tesorion
PewCrypt[47]	PewCrypt Autor

Literaturangaben

1. "Washington idle as ransomware ravages cities big and small" 28. September, 2019. Politico. https://www.politico.com/news/2019/09/28/ransomware-cities-washington-007376

2. "What you – and your company – should know about cyber insurance", 20. August, 2019. Talos. https://blog.talosintelligence.com/2019/08/cyber-insurance-FAQs.html

3. "The State of Ransomware in 2019" 17. Juni, 2019. IT Pro Today. https://www.itprotoday.com/threat-management/state-ransomware-2019

4. "California City Confirms Phone Line and Financial Data System Disruptions Caused by Ransomware". 2. August, 2019. Trend Micro. https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/california-city-confirms-phone-line-and-financial-data-system-disruptions-caused-by-ransomware

5. "Coordinated Ransomware Attack Cripples Local Government Organizations in Texas", 19. August, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/coordinated-ransomware-attack-cripples-local-government-organizations-in-texas

6 "The State of Ransomware in the US: Report and Statistics 2019". 12. Dezember, 2019. EMSISOFT blog. https://blog.emsisoft.com/en/34822/the-state-of-ransomware-in-the-us-report-and-statistics-2019/

7. "Alabama hospitals have been hit by a massive ransomware attack" 3. Oktober, 2019. https://www.foxnews.com/tech/alabama-hospitals-ransomware-attack

8. "500+ Schools Have Been Affected by Ransomware in 2019", 4. Oktober, 2019. Campus Safety, https://www.campussafetymagazine.com/safety/500-schools-ransomware-2019/

9. "Latest Quarterly Threat Report - Q1 2019" 2019. Proof Point. https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

10. "Proofpoint Q2 2019 Threat Report - Emotet's hiatus, mainstream impostor techniques, and more". 19. September, 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q2-2019-threat-report-emotets-hiatus-mainstream-impostor-techniques

11. "6 of the Biggest Cybersecurity Crises of 2019 (So Far)" 24. September, 2019. EC-Council Blog. https://blog.eccouncil.org/6-of-the-biggest-cybersecurity-crises-of-2019-so-far/

12. "Ransomware Attacks Double in 2019: Medical Providers Can't Recover and Shut Down" 3. Oktober, 2019. https://www.natlawreview.com/article/ransomware-attacks-double-2019-medical-providers-can-t-recover-and-shut-down

13. "Michigan's Brookside ENT and Hearing Center forced to close due to a Ransomware Attack" 23. April, 2019. SPAM Fighter. https://www.spamfighter.com/News-22154-Michigans-Brookside-ENT-and-Hearing-Center-forced-to-close-due-to-a-Ransomware-Attack.htm

14. "Victorian hospitals across Gippsland, Geelong and Warrnambool hit by ransomware attack". 1. Oktober, 2019. https://www.abc.net.au/news/2019-10-01/victorian-health-services-targeted-by-ransomware-attack/11562988?nw=0

15. "Ransomware Attack Affects 300,000 Patients in Utah". 12. September, 2019. CISO Mag. https://www.cisomag.com/ransomware-attack-affects-300000-patients-in-utah/

16. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks". 27. August, 2019 ProPublica. https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

17. "CYBER THREATSCAPE REPORT". 2019. Accenture. https://www.accenture.com/_acnmedia/pdf-107/accenture-security-cyber.pdf

18. "Ransomware Amounts Rise 3x in Q2 as Ryuk & Sodinokibi Spread". 2019. Coveware. https://www.coveware.com/blog/2019/7/15/ransomware-amounts-rise-3x-in-q2-as-ryuk-amp-sodinokibi-spread

19. "Armor Identifies 15 New Ransomware Victims in the Last 2 Weeks, All of them Educational Institutions – Threat Intelligence". 20. September, 2019. Armor. https://www.armor.com/resources/armor-identifies-10-new-ransomware-victims-in-the-past-9-days/

20. "4 Ransomware Trends to Watch in 2019". 13. Februar, 2019 https://www.recordedfuture.com/ransomware-trends-2019/

21. "BDO Cyber Threat Insights - 2019 2nd Quarter Report", July 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

22. "BDO's Fall 2019 Cyber Threat Report: Focus on Healthcare". Oktober 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdos-fall-2019-cyber-threat-report-focus-on-health

23. "Healthcare Cyber Heists in 2019" 3. Oktober, 2019. VMWare. https://www.carbonblack.com/resources/threat-research/healthcare-cyber-heists-in-2019/

24. "Australia | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/australia-global-threat-report-defender-power-on-the-rise/

25. "France | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/france-global-threat-report-defender-power-on-the-rise/

26. "Italy | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/italy-global-threat-report-defender-power-on-the-rise/

27. "Japan | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/japan-global-threat-report-defender-power-on-the-rise/

28. "Canada | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/canada-global-threat-report-defender-power-on-the-rise/

29. "Singapore | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/singapore-global-threat-report-defender-power-on-the-rise/

30. "UK | Global Threat Report | Defender Power On The Rise". 2019. VMWARE. https://www.carbonblack.com/land/uk-global-threat-report-defender-power-on-the-rise/

31. "Anticipating the Unknowns". März 2019. Cisco. https://ebooks.cisco.com/story/anticipating-unknowns/

32. "2020 Data Breach Investigations Report" 2020. Verizon. https://enterprise.verizon.com/resources/reports/dbir/

33. "IBM Security Study: Taxpayers Oppose Local Governments Paying Hackers in Ransomware Attacks". 5. September, 2019. IBM. https://newsroom.ibm.com/2019-09-05-IBM-Security-Study-Taxpayers-Oppose-Local-Governments-Paying-Hackers-in-Ransomware-Attacks

34. IT threat evolution Q2 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/

35. IT threat evolution Q1 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q1-2019-statistics/90916/

36. "The state of industrial cybersecurity". Juli 2019. Kaspersky. https://ics.kaspersky.com/media/2019_Kaspersky_ARC_ICS_report.pdf

37. "2019 Cyberthreat Defense Report" Cyber Edge Group. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

38. "Evasive Threats, Pervasive Effects". 27. August, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/evasive-threats-pervasive-effects

39. IT threat evolution Q3 2019 statistics" 2019 Kaspersky, https://securelist.com/it-threat-evolution-q3-2019-statistics/95269/

40. "What You Need to Know About the LockerGoga Ransomware." 20. März, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/what-you-need-to-know-about-the-lockergoga-ransomware/

41. "BDO Cyber Threat Insights - 2019 2nd Quarter Report", July 2019. BDO. https://www.bdo.com/insights/business-financial-advisory/cybersecurity/bdo-cyber-threat-insights-2019-2nd-quarter-report

Literaturangaben

42. Ransomware DecryptorTools, Kapersky https://noransom.kaspersky.com/

43. "ENISA Threat Landscape Report 2018". 28. Januar, 2019. ENISA. https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

44. "New GandCrab v5.1 Decryptor Available Now", 19. Februar, 2019. Bitdefender LABS. https://labs.bitdefender.com/2019/02/new-gandcrab-v5-1-decryptor-available-now/

45. "10 Ransomware Attacks You Should Know About in 2019" 28. April, 2019. Allot. https://www.allot.com/blog/10-ransomware-attacks-2019/

46. Ransomware DecryptorTools. Avast. https://www.avast.com/ransomware-decryption-tools

47. PewCrypt Ransomware Source. GitHub. https://github.com/000JustMe/PewCrypt

48. "Are the REvil, GranCrab Ransomware Families Related?" 25. September, 2019. MSSP Alert. https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/revil-gandcrab-related/

49. "Threat Landscape Report", Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q3-2019.pdf

50. "Sodin Ransomware includes exploit for Windows CVE-2018-8453 bug". 4. Juli, 2019. Security Affairs. https://securityaffairs.co/wordpress/87944/malware/sodin-ransomware-cve-2018-8453.html

51. "Threat Landscape Report" 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-report-q2-2019.pdf

52. "Emsisoft Decryptor for Aurora" 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/aurora

53. "Emsisoft Decryptor for Muhstik" 2019. Emsisoft. https://www.emsisoft.com/ransomware-decryption-tools/muhstik

54. "Caution! Ryuk Ransomware decryptor damages larger files, even if you pay". 9. Dezember, 2019. Emsisoft. https://blog.emsisoft.com/en/35023/bug-in-latest-ryuk-decryptor-may-cause-data-loss/

55. "RakhniDecryptor tool for defending against Trojan-Ransom.Win32.Rakhni ransomware". Kaspersky. https://support.kaspersky.com/10556

56. "Another two bite the dust: Kaspersky updates decryption tool to fight ransomware pair". 27. September, 2019. The Online Citizen. https://www.theonlinecitizen.com/2019/09/27/another-two-bite-the-dust-kaspersky-updates-decryption-tool-to-fight-ransomware-pair/

57. "Mira Ransomware Decryptor" 1. April, 2019. F-Secure. https://blog.f-secure.com/mira-ransomware-decryptor/

58. "Nemty update: decryptors for Nemty 1.5 and 1.6" Tesorion. https://www.tesorion.nl/nemty-update-decryptors-for-nemty-1-5-and-1-6/

59. "McAfee Labs Threats Report", August, 2019. McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf

60. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/2

61. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/3

62. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/6

63. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/7

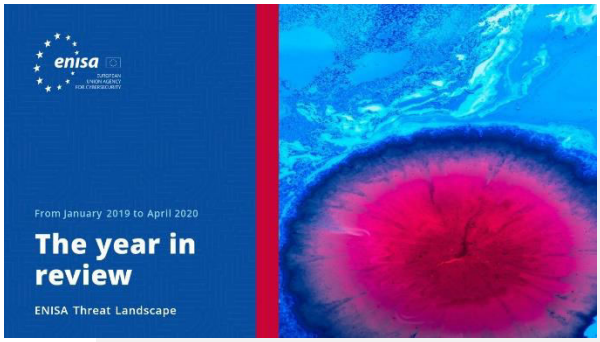
64. "The 10 biggest ransomware attacks of 2019" CRN. https://www.cm.com/slide-shows/security/the-10-biggest-ransomware-attacks-of-2019/11

65. https://www.nomoreransom.org/

„CTI hat sich im Bereich Cybersicherheit als wesentliches Instrument zur Verbesserung der Agilität und Effizienz bei der Verteidigung von Cyberangriffen fest etabliert.“

In ETL 2020

Themenbezogen



ENISA Threat Landscape Bericht **Das Berichtsjahr**

Eine Zusammenfassung der Cybersicherheitstrends für den Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Liste der 15 größten Bedrohungen**

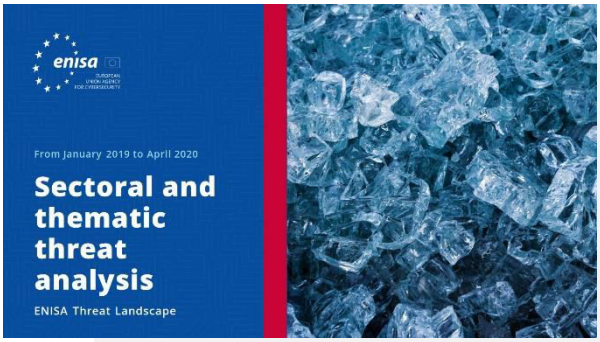
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht **Forschungsthemen**

Empfehlungen zu Forschungsthemen aus verschiedenen Quadranten der Cybersicherheit und Cyber Threat Intelligence.

LESEN SIE DEN BERICHT



LESEN SIE DEN BERICHT

ENISA Threat Landscape-Bericht
Sektorale und thematische Bedrohungsanalyse

Kontextualisierte Bedrohungsanalyse zwischen Januar 2019 und April 2020.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Aufkommende Trends

Die bedeutendsten Cybersicherheitstrends, die zwischen Januar 2019 und April 2020 beobachtet wurden.

LESEN SIE DEN BERICHT

ENISA Threat Landscape Bericht
Übersicht über Cyber Threat Intelligence

Der aktuelle Stand der Cyber Threat Intelligence in der EU.

Über

_ Die Agentur

Die Agentur der Europäischen Union für Cybersicherheit, ENISA, hat die Aufgabe, zu einer hohen Cybersicherheit innerhalb der Union beizutragen. Die Agentur der Europäischen Union für Cybersicherheit wurde 2004 gegründet und durch das EU-Gesetz zur Cybersicherheit gestärkt. Sie trägt zur Unionspolitik im Bereich der Cybersicherheit bei, erhöht die Vertrauenswürdigkeit von ICT-Produkten, -Diensten und -Prozessen durch Programme für die Cybersicherheitszertifizierung, sie kooperiert mit den Mitgliedstaaten und Organen der EU und unterstützt Europa dabei, sich den künftigen Herausforderungen im Bereich der Cybersicherheit zu stellen. Durch Wissensaustausch, Aufbau von Fähigkeiten und Sensibilisierung in Bezug auf Cybersicherheit arbeitet die Agentur gemeinsam mit ihren wichtigsten Interessenträgern darauf hin, das Vertrauen in die vernetzte Wirtschaft zu stärken, die Infrastruktur der Union abwehrfähiger zu machen und schließlich ein sicheres digitales Umfeld für die Gesellschaft und die Bürger Europas zu gewährleisten. Weitere Information über die ENISA und ihre Arbeit finden Sie unter www.enisa.europa.eu.

Mitwirkende

Christos Douligeris, Omid Raghimi, Marco Barros Lourenço (ENISA), Louis Marinos (ENISA) und *alle Mitglieder der ENISA CTI Interessenvertreter:* Andreas Sfakianakis, Christian Doerr, Jart Armin, Marco Riccardi, Mees Wim, Neil Thaker, Pasquale Stirparo, Paul Samwel, Pierluigi Paganini, Shin Adachi, Stavros Lingris (CERT EU) und Thomas Hemker.

Herausgeber

Marco Barros Lourenço (ENISA) und Louis Marinos (ENISA).

Kontaktangaben

Für Fragen über dieses Dokument, verwenden Sie bitte enisa.threat.information@enisa.europa.eu.
Für Medienanfragen zu dieser Stellungnahme verwenden Sie bitte die folgenden Kontaktangaben: press@enisa.europa.eu.

Wir würden gerne Ihr Feedback zu diesem Bericht erhalten!
Bitte nehmen Sie sich einen Moment Zeit, um den Fragebogen auszufüllen. Um das Formular zu öffnen, können Sie hier klicken.

Impressum/Rechtshinweise

Sofern nichts anderes angegeben ist, gibt diese Veröffentlichung die Ansichten und Auslegungen der ENISA wieder. Diese Veröffentlichung ist nicht als eine Maßnahme der ENISA oder ihrer Gremien auszulegen, sofern sie nicht gemäß der Verordnung (EU) Nr. 526/2013 angenommen wurde. Diese Veröffentlichung entspricht nicht unbedingt dem neuesten Stand und kann in angemessenen Abständen aktualisiert werden.

Quellen von Dritten werden zitiert, sofern erforderlich. Die ENISA haftet nicht für den Inhalt der externen Quellen, einschließlich externer Websites, auf die in dieser Veröffentlichung verwiesen wird.

Die vorliegende Veröffentlichung ist nur für Informationszwecke gedacht. Sie muss kostenlos zugänglich sein. Weder die ENISA noch in deren Namen oder Auftrag tätige Personen können für die Nutzung der in dieser Veröffentlichung enthaltenen Informationen haftbar gemacht werden.

ISBN: 978-92-9204-354-4
DOI: 10.2824/552242

Vasilissis Sofias Str 1, Maroussi 151 24, Attiki, Griechenland
Tel.: +30 28 14 40 9711
info@enisa.europa.eu
www.enisa.europa.eu

https://www.enisa.europa.eu