enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Phishing

ENISA Threat Landscape

Überblick

Phishing ist der betrügerische Versuch, Benutzerdaten wie Anmelde-, Kreditkarteninformationen oder sogar Geld mithilfe von Social-Engineering-Techniken zu stehlen. **Diese Art von Angriff wird normalerweise über E-Mail-Nachrichten gestartet, die anscheinend von einer seriösen Quelle gesendet werden, um den Benutzer davon zu überzeugen, einen schadhaften Anhang zu öffnen oder einer betrügerischen URL zu folgen.** Eine gezielte Form von Phishing, die als „Spear Phishing" bezeichnet wird, beruht auf Vorabuntersuchungen der Opfer, damit der Betrug authentischer erscheint und damit zu einer der erfolgreichsten Arten von Angriffen auf Unternehmensnetzwerke wird.[1]

Eine emotionale Reaktion rechtfertigt die Handlungen vieler Menschen, wenn sie Phishing zum Opfer fallen, und das ist genau das, wonach Hacker suchen. In einem Trainingskontext sollte dies mit einer Phishing-Simulation erreicht werden. Die Schulung von E-Mail-Benutzern ist eine der häufig verwendeten Maßnahmen zur Verhinderung von Phishing. Die Ergebnisse sind jedoch nicht überzeugend, da Bedrohungsakteure ihre Arbeitsweise ständig ändern. Der domänenbasierte Standard für Nachrichtenauthentifizierung, Berichterstellung und Konformität (DMARC) stellt sicher, dass E-Mails von betrügerischen Domains blockiert werden, was die Erfolgsrate von Phishing-, Spoofing- und Spam-Angriffen verringert.

E-Mail ist auch in Zukunft der wichtigste Mechanismus für Phishing, aber nicht mehr lange. Wir sehen bereits eine Zunahme der Verwendung von Social Media Messaging, WhatsApp und anderen, um Angriffe durchzuführen. Die wichtigste Änderung betrifft die Methoden zum Senden der Nachrichten, die mit der Einführung der gegnerischen künstlichen Intelligenz (KI) zur Vorbereitung und zum Senden der Nachrichten komplexer werden. Phishing und Spear Phishing sind wichtige Angriffsmethoden für andere Bedrohungen, z. B. unbeabsichtigte Insider-Bedrohungen.

Erkenntnisse

26,2_ **Milliarden an Verlusten im Jahr 2019 durch Business E-Mail Kompromittierung (BEC) Angriffe**[20]

42,8 %_ **aller schadhaften Anhänge waren Microsoft Office-Dokumente**[25]

667 %_ **Zunahme der Phishing-Betrügereien in nur einem Monat während der COVID-19-Pandemie**[6]

30 %_ **der Phishing-Nachrichten gingen an einem Montag ein**[29]

32,5 %_ **aller E-Mail benutzten das Schlüsselwort „Zahlung“ in der Betreffzeile**[28]

Kill chain

Schritt des Angriffs-Workflows

Umfang des Zwecks

Installation

Command & Control

Zielführende Maßnahmen

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

Entwicklungen

_Die am häufigsten verwendeten Arten von Dienstleistungen sind Webmail und Software-as-a-Service

Nach einigen Prognosen übertrafen Phishing-Angriffe auf Software-as-a-Service- (SaaS) und Webmail-Dienste erstmals im ersten Quartal 2019 die Angriffe auf Zahlungsdienste und machten sie mit 36 % aller Phishing-Angriffe zum am stärksten betroffenen Sektor.[2] Dieser neue Rekord folgt dem Trend von 2018, als SaaS- und Webmail-Dienste gerade den Finanzsektor überholt hatten[3]. Obwohl die Zahl bis Ende 2019 auf 30,8 % gesunken war, standen die oben genannten Dienste weiterhin ganz oben auf der Liste[2,3], wobei **Microsoft 365-Dienste das Hauptziel der Phisher waren.**[4]

_Business E-Mail Kompromittierung (BEC) -Angriffe waren weiterhin ein Problem

Eine kürzlich durchgeführte Studie ergab, dass 88 % der weltweiten Organisationen Spear-Phishing-Angriffe erlebten und 86 % BEC-Angriffen ausgesetzt waren.[16] Im Jahr 2019 war Microsoft 365 einer der am meisten anvisierten Dienste, und der Schwerpunkt lag auf der Erlangung von Anmeldedaten.[17] Sobald diese Anmeldedaten entwendet waren, konnte der Angreifer mehr Organisationsdaten sammeln. Dieser Prozess konnte Wochen oder Monate dauern (18) und dann zu Spear-Phishing-Angriffen führen. Der Angreifer gab sich als Mitarbeiter, Chief Executive Officer (CEO) oder sogar als vertrauenswürdiger Lieferant aus, um Gelder umzuleiten oder Zahlungen auf Konten von Drittanbietern umzuleiten.[14] Im ersten Quartal 2019 waren Unternehmen 120 % häufiger als ein Jahr zuvor von BEC-Angriffen betroffen[19], was zu Verlusten von bis zu 26,2 Milliarden USD (ca. 22,2 Milliarden EUR) führte.[20]

_Mehr als zwei Drittel der Phishing-Sites haben HTTPS genutzt

In den letzten Jahren hat die Anzahl der Phishing-Seiten, die HTTPS eingeführt haben, stark zugenommen[13]. Im letzten Quartal 2019 verwendeten 74 % der Phishing-Sites HTTPS[32], ein deutlicher Anstieg gegenüber nur 32 % vor zwei Jahren. Obwohl Technologien wie HTTPS und SSL die Kommunikation zwischen einem Kunden und einem Server sichern sollen, kann das Vorhandensein einer Sperre in einem Symbol in der Adressleiste des Browsers die Illusion erzeugen, dass einer Website vertraut werden kann.

Bedrohungsakteure können auch legitime Websites verwenden, die sie gehackt haben, um Phishing-Inhalte zu hosten. Daher ist es für den Endbenutzer schwierig, eine Website als unsicher zu identifizieren[14]. Weitere Faktoren, die zu dem starken Anstieg der HTTPS-Nutzung beitragen, sind die Vielzahl kostenloser Zertifikatdienste wie Let's Encryp[15] und die Tatsache, dass moderne Browser jede HTTPS-Seite ohne weitere Überprüfungen als sicher markieren.

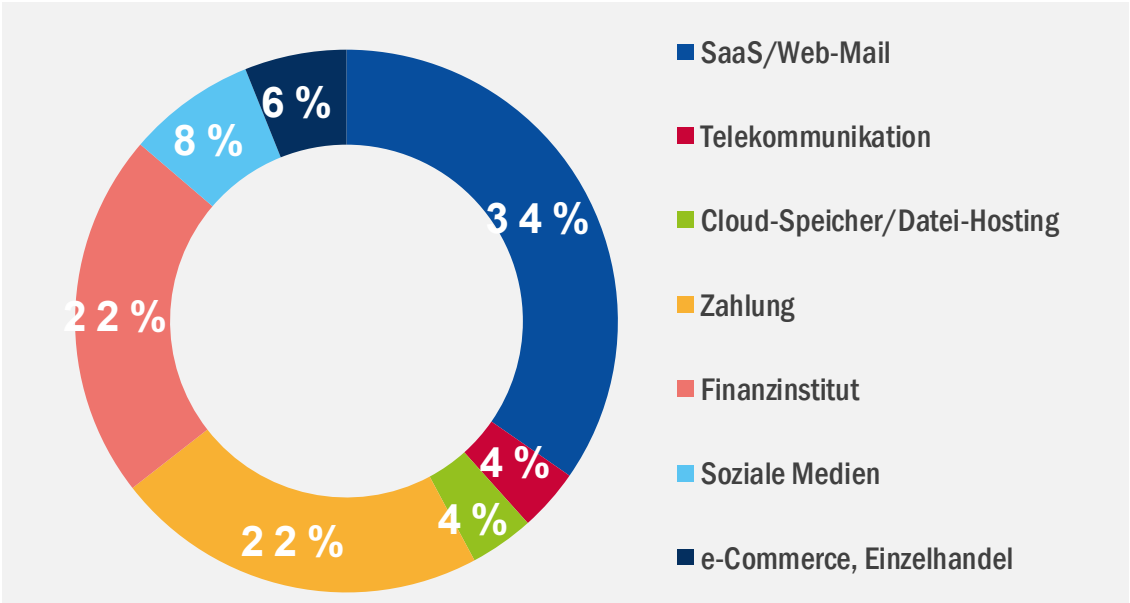


Abbildung 1: Pishing-Angriffsziele. Quelle: Proof Point[32]

Entwicklungen

_Phishing-as-a-Service (PhaaS) im Aufmarsch

Diese Arten von Diensten basieren in der Regel auf Abonnements oder in Form eines Kits, das gegen eine Gebühr heruntergeladen werden kann, und beseitigen die technologischen Eintrittsbarrieren, sodass auch weniger technisch versierte Personen einen gezielten Angriff ausführen können. In einem Bericht eines Sicherheitsforschers[21] wurden 5.334 einzigartige Phishing-Sets identifiziert, die bis Juni 2019 erhältlich waren. Noch besorgniserregender waren die relativ geringen Kosten dieser Lösungen, etwa 50 bis 80 USD für ein monatliches Abonnement. In demselben Bericht wurde angegeben, dass 87 % der Sets Ausweichmechanismen wie HTML-Zeichencodierung und Inhaltsverschlüsselung enthielten. Interessanterweise wurden einige dieser Dienste auf legitimen Cloud-Diensten mit geeigneten DNS-Namen und -Zertifikaten (Domain Name System) gehostet. Statistiken von nur einem dieser Dark-Netz-Marktplätze zeigen, wie erfolgreich diese Angriffe es dem Angreifer oder der Gruppe ermöglichen, etwa 65.000 Konten pro Monat zu stehlen.[22]

_Trends in Bezug auf Vorfälle

- Die Effektivität von Phishing-Angriffen mithilfe von Cloud-Speicher-, DocuSign- und Microsoft-Cloud-Diensten hat sich geändert.
- Zu den Betrugsangriffen gehören Programme wie Business E-Mail Kompromittierung (BEC) und Identitätsbetrugstechniken, die auf Social Engineering basieren, um Phishing-Kampagnen effektiver zu gestalten.
- Phishing von Microsoft 365-Diensten war das Hauptschema, aber der Schwerpunkt liegt weiterhin auf dem Sammeln von Anmeldedaten.
- Über 99 % der E-Mails, die Malware verbreiten, erforderten menschliches Eingreifen - Folgen von Links, Öffnen von Dokumenten, Akzeptieren von Sicherheitswarnungen und anderen Handlungen -, um wirksam zu sein.[44]

Top-Phishing-Themen im Jahr 2019

- Generisches Ernten von E-Mail-Anmeldedaten
- Phishing von Office 365-Konten
- Phishing von Finanzinstituten
- Microsoft OWA Phishing
- OneDrive Phishing
- American Express Phishing
- Chalbhai Generic Phishing
- Adobe Account Phishing
- Docusign Phishing
- Netflix Phishing
- Phishing von Dropbox-Konten
- Phishing von LinkedIn-Konten
- Apple Account Phishing
- Phishing der Post/des Versands
- Microsoft Online Document Phishing (Excel und Word)
- Phishing von Windows-Einstellungen
- Google Drive Phishing
- PayPal Phishing

Quelle: Proof Point[32]

Entwicklungen

_COVID-19 wird als Phishing-Köderverwendet

Cyberkriminelle nutzen die öffentliche Angst vor der COVID-19-Pandemie, die erstmals Ende 2019 auftrat. Es wurde berichtet, dass Phishing-Angriffe mit dem Virus innerhalb eines Monats (zwischen Ende Februar 2020 und Ende März 2020) um 667 % zunahmen, und diese Masche allein machte beachtliche 2 % aller Phishing-Betrugsfälle aus.[5]

Bei neuen Betrügereien handelte es sich um Phishing-E-Mails, die so aussehen sollten, als stammten sie vom US-amerikanischen Zentrum für Krankheitskontrolle (CDC)[6], der Weltgesundheitsorganisation[7] oder sogar von Teams einer Uniklinik[8]. Sie behaupteten entweder fälschlicherweise, Infektionsfälle im Bereich des Opfers zu zeigen, oder teilten die Meinungen von medizinischen Experten, um das Opfer dazu zu verleiten, einem böswilligen Link zu folgen. Aus diesem Grund haben das FBI und die WHO Warnungen herausgegeben[8,9] Da viele Menschen in Quarantäne von zu Hause aus arbeiteten und häufig veraltete Sicherheitssysteme verwendeten[11], versuchten Cyberkriminelle, aufkommende Chancen und Schwachstellen auszunutzen[12].

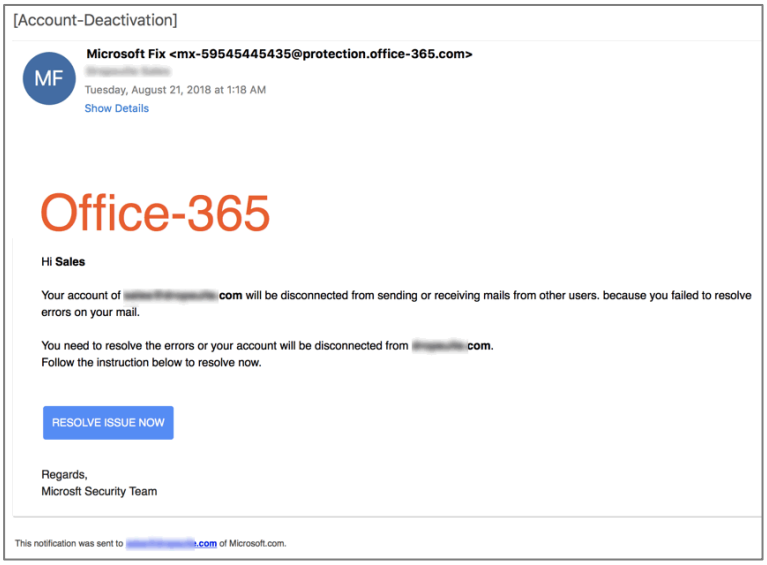


Abbildung 2: Office 365 Phishing E-Mail, Credit Dropsuite[45]

Reaktion der ENISA auf die COVID-19-Pandemie

Der Ausbruch von COVID-19 hat die Art und Weise, wie wir unser Leben führen, immens verändert. In dieser zunehmend vernetzten Welt können wir glücklicherweise unser berufliches und privates Leben virtuell fortsetzen. In dieser beispiellosen Zeit teilte die EU-Agentur für Cybersicherheit (ENISA) ihre Empfehlungen zur Cybersicherheit[46] zu verschiedenen Themen mit, darunter Telearbeit, Online-Shopping und E-Health sowie Aktualisierungen der wichtigsten Sicherheitsratschläge, die auf die betroffenen Sektoren zugeschnitten sind. ENISA überprüft die Bedrohungslandschaft während der Pandemie und gibt Ratschläge, wie die Risiken der kritischsten Bedrohungen gemindert werden können. Besonderes Augenmerk wird auf Phishing gelegt, da die Anzahl der Angriffe zunimmt.

Abbildung 3: ENISA YouTube-Video zu COVID-19. Quelle ENISA

Vorfälle

Zielbranchen

Der Gesundheitssektor war 2019 stark von Phishing- (oder Spear-Phishing-) Angriffen betroffen. Ein Sicherheitsforscher[42] betrachtete Phishing als den Hauptangriffsvektor des Jahres, über den Einsatz von Social-Engineering-Taktiken, um mit Malware[7] infizierte E-Mails oder Links zu infizierten Websites zu versenden. Andere Sektoren waren ebenfalls von Phishing-Angriffen betroffen, beispielsweise Regierungen und andere Einrichtungen der öffentlichen Verwaltung. Beispielsweise erhielten im November und Dezember 2019 mehrere Diplomaten und Beamte der ukrainischen Regierung Spear-Phishing-E-Mails, mit denen sie an kompromittierte Websites weitergeleitet wurden.[43]

Angriffsvektoren

Spear Phishing ist nach wie vor eine äußerst verbreitete Technik für den Erstzugriff, die von böswilligen Akteuren verwendet wird. Diese verwenden eine Vielzahl von Social-Engineering-Taktiken, um Empfänger dazu zu bewegen, Anhänge zu öffnen oder zu einer infizierten Website zu navigieren. Spear-Phishing-Nachrichten enthalten normalerweise schädliche makroaktivierte Microsoft Office-Dokumente oder einen Link zu solchen Dokumenten. Nachdem ein Benutzer „Inhalt aktivieren" ausgewählt hat, beginnt das eingebettete Makro normalerweise mit der Ausführung einer Kette von verschleierten Skripten, die letztendlich zum Herunterladen von Malware der ersten Stufe oder von Dropper führen. JavaScript und PowerShell scheinen für diesen Zweck die beliebtesten Skriptsprachen zu bleiben.

Beispiele

- Ein Phishing-Angriff auf Studenten der Lancaster University führte zum Verlust personenbezogener Daten[37]
- Hacker haben Anmeldedaten von 2500 Discord-Benutzern gephished[38]
- Online-Fitnessdienstleister Opfer eines Phishing-Angriffs[39]
- Patienten wurden von einem UConn Health Phishing-Angriff betroffen[41]
- Eine Tochtergesellschaft eines Autoherstellers verlor 37 Millionen USD (ca. 31 Millionen EUR) aufgrund eines BEC-Betrugs[33]

Minderung

Vorgeschlagene Maßnahmen

- Informieren Sie die Mitarbeiter, um gefälschte und böswillige E-Mails zu identifizieren und wachsam zu bleiben. Starten Sie simulierte Phishing-Kampagnen, um die Infrastruktur des Unternehmens sowie die Reaktionsfähigkeit der Mitarbeiter zu testen.
- Erwägen Sie die Verwendung eines Sicherheits-E-Mail-Gateways mit regelmäßiger (möglicherweise automatisierter) Wartung von Filtern (Anti-Spam, Anti-Malware, richtlinienbasierte Filterung).
- Erwägen Sie die Anwendung von Sicherheitslösungen, die maschinelles Lernen verwenden, um Phishing-Sites in Echtzeit zu identifizieren.
- Deaktivieren Sie die automatische Ausführung von Code, Makros, das Rendern von Grafiken und das Vorladen von per E-Mail gesendeten Links auf den E-Mail-Clients und aktualisieren Sie diese regelmäßig.
- Implementieren Sie einen der Standards zur Reduzierung von Spam-E-Mails: SPF (Sender Policy Framework)[34], DMARC (Domain-basierte Nachrichtenauthentifizierung, Berichterstellung & Konformität)[35] und DKIM (Domain Keys Identified Mail).[36]
- Verwenden Sie im Idealfall eine sichere E-Mail-Kommunikation mit digitalen Signaturen oder Verschlüsselung, für kritische finanzielle Transaktionen oder beim Austausch vertraulicher Informationen.
- Implementieren Sie die Erkennung von Betrug und Anomalien auf Netzwerkebene für eingehende und ausgehende E-Mails.
- Vermeiden Sie das Klicken auf zufällige Links, insbesondere auf kurze Links in sozialen Medien.
- Klicken Sie nicht auf Links oder laden Sie keine Anhänge herunter, wenn Sie sich über die Quelle einer E-Mail nicht sicher sind.

- Vermeiden Sie es, personenbezogene Informationen in sozialen Medien zu teilen, z. Dauer der Abwesenheit von Büro oder Zuhause, Fluginformationen usw., da diese von Bedrohungsakteuren aktiv genutzt werden, um Informationen über ihre Ziele zu sammeln.
- Überprüfen Sie den Domainnamen der von Ihnen besuchten Websites auf Tippfehler, insbesondere bei Namen vertraulicher Websites, z. B. Bank-Websites. Bedrohungsakteure registrieren normalerweise gefälschte Domains, die legitimen Domains ähneln, und verwenden sie, um ihre Ziele zu „phischen". Es reicht nicht aus, nur auf eine HTTPS-Verbindung zu achten.
- Aktivieren Sie gegebenenfalls die Zwei-Faktor-Authentifizierung, um Kontoübernahmen zu verhindern.
- Verwenden Sie für jeden Onlinedienst ein sicheres und eindeutiges Passwort. Die Wiederverwendung des gleichen Passworts für verschiedene Dienste ist ein ernstes Sicherheitsproblem und sollte jederzeit vermieden werden. Die Verwendung starker und eindeutiger Anmeldedaten für jeden Onlinedienst begrenzt das Risiko einer möglichen Kontoübernahme nur auf den betroffenen Dienst. Die Verwendung einer Passwort-Manager-Software erleichtert die Verwaltung aller Passwörter.
- Wenn Sie Geld auf ein Konto überweisen, überprüfen Sie die Informationen des Bankempfängers über ein anderes Medium. Unverschlüsselte und nicht signierte E-Mails sollten nicht als vertrauenswürdig eingestuft werden, insbesondere für sensible Anwendungsfälle wie diesen.
- Überprüfen Sie, wie Kontakt-, Registrierungs-, Abonnement- und Feedbackformulare auf Ihrer Website funktionieren, und fügen Sie gegebenenfalls Überprüfungsregeln hinzu, damit diese nicht von Angreifern ausgenutzt werden können.

Literaturangaben

1. "What Is Phishing?". Cisco. https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

2. "Phishing Activity Trends Report Q1". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

3. "2018 Phishing Trends & Intelligence Report" 2018. Phishlabs.

https://info.phishlabs.com/hubfs/2018%20PTI%20Report/PhishLabs%20Trend%20Report_2018-digital.pdf

4. "Microsoft remains phishers' #1 target for the fifth straight quarter" 22. August, 2019. Vade Secure.
https://www.vadesecure.com/en/phishers-favorites-q2-2019/

5. "Threat Spotlight: Coronavirus-Related Phishing". 26. März, 2020. https://blog.barracuda.com/2020/03/26/threat-spotlight-coronavirus-related-phishing/

6 "Coronavirus phishing emails: How to protect against COVID-19 scams" 2020. https://us.norton.com/internetsecurity-online-scams-coronavirus-phishing-scams.html

7. "Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer". 2020. IBM
https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As-HawkEye-Info-Stealer-2f9a23ad901ad94a8668731932ab5826

8. "Abnormal Attack Stories #6: Coronavirus Credential Theft" 13. März, 2020.
https://abnormalsecurity.com/blog/abnormal-attack-stories-6-coronavirus-credential-theft/

9. "FBI Sees Rise in Fraud Schemes Related to the Coronavirus (COVID-19) Pandemic". 20. März, 2020. FBI:
https://www.ic3.gov/media/2020/200320.aspx

10. "Beware of criminals pretending to be WHO". 2020. WHO https://www.who.int/about/communications/cyber-security

11. "Global police agencies issue alerts on Covid-related cyber-crime". 6. April, 2020. SC Magazine.
https://www.scmagazineuk.com/global-police-agencies-issue-alerts-covid-related-cyber-crime/article/1679473

12. "Catching the virus cybercrime, disinformation and the COVID-19 pandemic". 3. April, 2020. EUROPOL.
https://www.europol.europa.eu/publications-documents/catching-virus-cybercrime-disinformation-and-covid-19-pandemic

13. "New FireEye Email Threat Report Reveals Increase in Social Engineering Attacks". 25. Juni, 2019. FireEye.
https://www.fireeye.com/company/press-releases/2019/new-fireeye-email-threat-report-reveals-increase-in-social-engin.html

14. "HTTPS Protocol Now Used in 58% of Phishing Websites". 24. Juni, 2019. Trend Micro.
https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/https-protocol-now-used-in-58-of-phishing-websites

15. Let's Encrypt. https://letsencrypt.org/

16. "2020 'State of the Phish': Security Awareness Training, Email Reporting More Critical as Targeted Attacks Spike". 23. Januar, 2020. Proof Point. https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical

17. "Human factor report". 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

18. "Phishing Activity Trends Report Q3". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q3_2019.pdf

19. "Business Email Compromise Results in $26B in Losses Over the Last Three Years". 12. September, 2019. Proof Point. https://www.proofpoint.com/us/corporate-blog/post/business-email-compromise-results-26b-losses-over-last-three-years

20. "Business Email Compromise The $26 Billion Scam" 10. September, 2019. FBI: https://www.ic3.gov/media/2019/190910.aspx

21. "Evasive Phishing Driven by Phishing-as-a-Service". 1. Juli, 2019. Cyren.

https://www.cyren.com/blog/articles/evasive-phishing-driven-by-phishing-as-a-service

22. "Phishing made easy: Time to rethink your prevention strategy?". 2016. Imperva. https://www.imperva.com/docs/Imperva-HII-phishing-made-easy.pdf

23. 3. Quartal 2019 Email Fraud and Identity Deception Trends". 2019. Agari. https://www.agari.com/insights/ebooks/2019-q3-report/

24. "FBI: BEC Losses Soared to $1.8 Billion in 2019". 12. Februar, 2020. Infosecurity Magazine. https://www.infosecurity-magazine.com/news/fbi-bec-losses-soared-to-18/

25. "Email: Click with Caution". Juni 2019. Cisco. https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

26. "Experts report a rampant growth in the number of malicious, lookalike domains". 18. November, 2019. https://securityaffairs.co/wordpress/94021/hacking/lookalike-domains-tls-certificate.html

27. "Proofpoint Q3 2019 Threat Report — Emotet's return, RATs reign supreme, and more". 7. November, 2019. Proof Point. https://www.proofpoint.com/us/threat-insight/post/proofpoint-q3-2019-threat-report-emotets-return-rats-reign-supreme-and-more

28. "Human Factor Report." 2019. Proof Point. https://www.proofpoint.com/sites/default/files/gtd-pfpt-us-tr-human-factor-2019.pdf

29. "2019 Phishing and fraud report" 2019. F5 Labs. https://www.f5.com/content/dam/f5-labs-v2/article/pdfs/F5Labs_2019_Phishing_and_Fraud_Report.pdf

30. "Report: Microsoft, PayPal, and Netflix Most Impersonated Brands in Phishing Attacks in Q1 2019" 8. Mai, 2019. Trend Micro. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/report-microsoft-paypal-and-netflix-most-impersonated-brands-in-phishing-attacks-in-q1-2019

31. "Spam and phishing in Q3 2019". 26. November, 2019. Kaspersky. https://securelist.com/spam-report-q3-2019/95177/

32. "Phishing Activity Trends Report". 2019. APWG. https://docs.apwg.org/reports/apwg_trends_report_q4_2019.pdf

33. "Toyota Subsidiary Loses $37 Million Due to BEC Scam" 20. September, 2019. CPO Magazine. https://www.cpomagazine.com/cyber-security/toyota-subsidiary-loses-37-million-due-to-bec-scam/

34. Open SPF. http://www.openspf.org/

35. "Domain-based Message Authentication, Reporting & Conformance". DMARC. https://dmarc.org/

Literaturangaben

36. "DomainKeys Identified Mail (DKIM)". DKIM. http://www.dkim.org/

37. "Cyber incident". 22. Juli, 2019. Lancaster University. https://www.lancaster.ac.uk/news/phishing-attack

38. "Hackers publish login credentials of 2500 Discord users" 22. Juli, 2019. Cyware Social. https://cyware.com/news/hackers-publish-login-credentials-of-2500-discord-users-8d3ea2c7

39. "Bodybuilding.com Breach: Proof That An Organization's Biggest Cyber Risk Is Its People" 24. April, 2019. Forbes. https://www.forbes.com/sites/jameshadley/2019/04/24/bodybuilding-com-breach-proof-that-an-organizations-biggest-cyber-risk-is-its-people/#1ea113751bef

40. "Phishing Attack Exposes 600k Health Records" 19. Juni, 2019. Secure World. https://www.secureworldexpo.com/industry-news/healthcare-data-breach-example-2019

41. "326,000 Patients Impacted in UConn Health Phishing Attack". 25. Februar, 2019 Health IT Security. https://healthitsecurity.com/news/326000-patients-impacted-in-uconn-health-phishing-attack

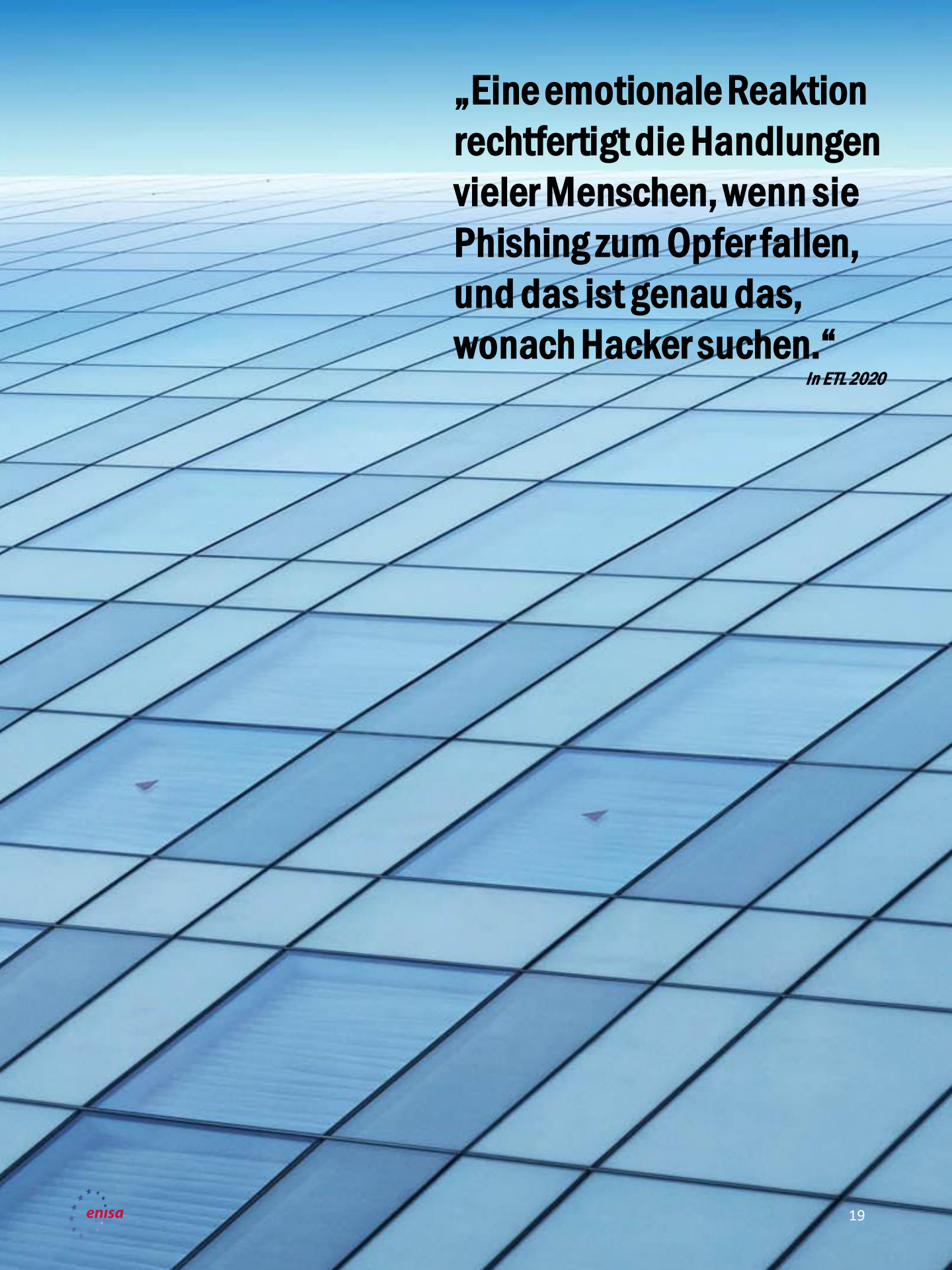
42. "Cybercrime Tactics and Techniques: the 2019 state of healthcare". 2019. Malwarebytes. https://resources.malwarebytes.com/resource/cybercrime-tactics-and-techniques-the-2019-state-of-healthcare/

43. "Significant Cyber Incidents". 2019. CSIS. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents

44. "More Than 99% of Cyberattacks Need Victims' Help". 9. September, 2019. Dark Reading. https://www.darkreading.com/cloud/more-than-99--of-cyberattacks-need-victims-help/d/d-id/1335769

45. "office-365-phishing-attacks-deconstructed" https://dropsuite.com/office-365-phishing-attacks-deconstructed/

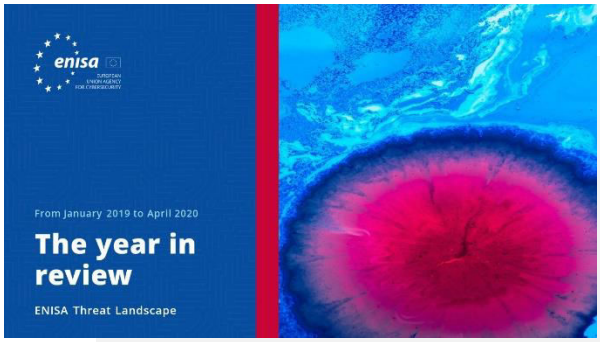
46. ENISA. https://www.enisa.europa.eu/topics/wfh-covid19



„Eine emotionale Reaktion rechtfertigt die Handlungen vieler Menschen, wenn sie Phishing zum Opfer fallen, und das ist genau das, wonach Hacker suchen.“

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**

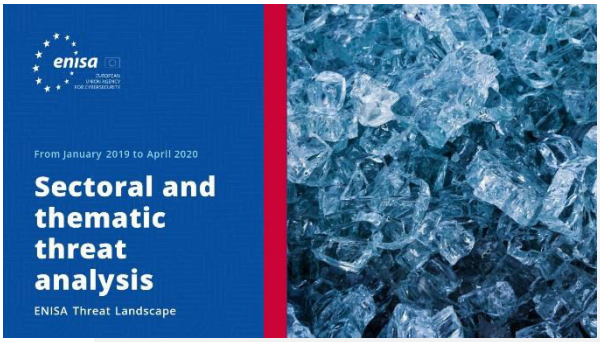
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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



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.

LESEN SIE DEN BERICHT

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

enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

https://www.enisa.europa.eu