enisa

EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

DE

Von Januar 2019 bis April 2020

Insider-bedrohung

ENISA Threat Landscape

Überblick

Eine Insider-Bedrohung ist eine Aktion, die zu einem Vorfall führen kann, die von jemandem oder einer Gruppe von Personen ausgeführt wird, die mit dem potenziellen Opfer verbunden sind oder für dieses arbeiten. Es gibt verschiedene Muster, die mit Bedrohungen von innen verbunden sind. Ein bekanntes Insider-Bedrohungsmuster (auch als „Missbrauch von Privilegien“ bezeichnet) tritt auf, wenn Außenstehende mit internen Akteuren zusammenarbeiten, um nicht genehmigten Zugriff auf Ressourcen zu erhalten. Insider können unbeabsichtigt durch Nachlässigkeit oder mangelndes Wissen Schaden anrichten. Da diese Insider häufig Vertrauen und Privilegien sowie Kenntnisse über die Organisationsrichtlinien, -prozesse und -verfahren der Organisation genießen, ist es schwierig, zwischen legitimem, böswilligem und fehlerhaftem Zugriff auf Anwendungen, Daten und Systeme zu unterscheiden.[1]

Die fünf Arten von Insider-Bedrohungen können anhand ihrer Gründe und Ziele definiert werden:

a) Nachlässige Mitarbeiter, die Daten falsch behandeln, Nutzungsrichtlinien brechen und nicht autorisierte Anwendungen installieren;

b) Insider-Agenten, die Informationen im Namen von Außenstehenden stehlen;

c) Verärgerte Mitarbeiter, die versuchen, ihrer Organisation Schaden zuzufügen;

d) Böswillige Insider, die vorhandene Privilegien nutzen, um Informationen zum persönlichen Vorteil zu stehlen;

e) Unbesonnene Dritte, die die Sicherheit durch Intelligenz, Missbrauch oder böswilligen Zugriff auf oder Nutzung eines Vermögenswerts gefährden.

Alle fünf Arten von Insider-Bedrohungen sollten kontinuierlich untersucht werden, da die Anerkennung ihrer Existenz und ihre Vorgehensweise die Strategie der Organisation für Sicherheit und Datenschutz definieren sollten.

Erkenntnisse

65 %_ der Auswirkungen von Insider-Bedrohungen betreffen Schäden an der Reputation und den Finanzen der Organisation[12]

88 %_ der befragten Organisationen erkennen an, dass Insider-Bedrohungen alarmierend sind[10]

€11,45_ sind die durchschnittlichen jährlichen Kosten für Cybersicherheitsvorfälle, die von einem Insider der Organisation verursacht werden[8]

40 %_ der befragten Organisationen fühlen sich anfällig für den Zugriff auf vertrauliche Geschäftsinformationen[11]

Kill chain

Insiderbedrohung

Ausspähung	Wappnung	Lieferung	Betreibung

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

Beschreibung

_Geld regiert die Welt

Aufgrund der steigenden Kosten anderer Angriffsmethoden sind Angreifer bereit, Insidern große Geldbeträge anzubieten. Der Preis für Insider hängt von der Position des Insiders im Unternehmen, dem Unternehmen selbst, der Art und Komplexität des angeforderten Dienstes, der Art der exfiltrierten Daten und dem Sicherheitsniveau im Unternehmen ab. Zu den Möglichkeiten, wie Angreifer Insider rekrutieren, gehören: (1) einfach ein Angebot in Foren veröffentlichen und eine Belohnung für bestimmte Informationen anbieten; (2) Verschleierung ihrer Handlungen, damit Mitarbeiter nicht erkennen, dass sie illegal handeln, persönliche Informationen offenlegen oder Insideraktivitäten durchführen; und (3) Erpressung.[4]

_Verdächtige Aktionen Urbi et Orbi

Ein ehemaliger Softwareentwickler eines Cloud-Dienstanbieters nutzte eine falsch konfigurierte Webanwendungs-Firewall und griff auf die Konten und Kreditkartendatensätze von mehr als 100 Millionen Kunden zu. Das Unternehmen hat die Sicherheitsanfälligkeit inzwischen behoben und festgestellt, dass keine Kreditkartenkontonummern oder Anmeldedaten kompromittiert wurden. Dieser Insider-Bedrohungsfall ist besonders interessant, da der ehemalige Mitarbeiter, der zum Hacker wurde, keine Angst hatte, die Identität zu verbergen. Der Hacker teilte die Hacking-Methode mit Kollegen von Capital One über einen Chat-Dienst. Der Hacker hat die Informationen auch auf GitHub gepostet (unter Verwendung des vollständigen Namens) und auch in den sozialen Medien damit geprahlt. Diese Art von Verhalten ist ein Phänomen, das Psychologen als „Leakage" bezeichnen, bei dem Insider, die planen, Schaden anzurichten, ihre Pläne offenlegen. Capital One geht davon aus, dass der Verstoß bis zu 150 Millionen USD (ca. 127 Millionen EUR) kosten wird.[5]

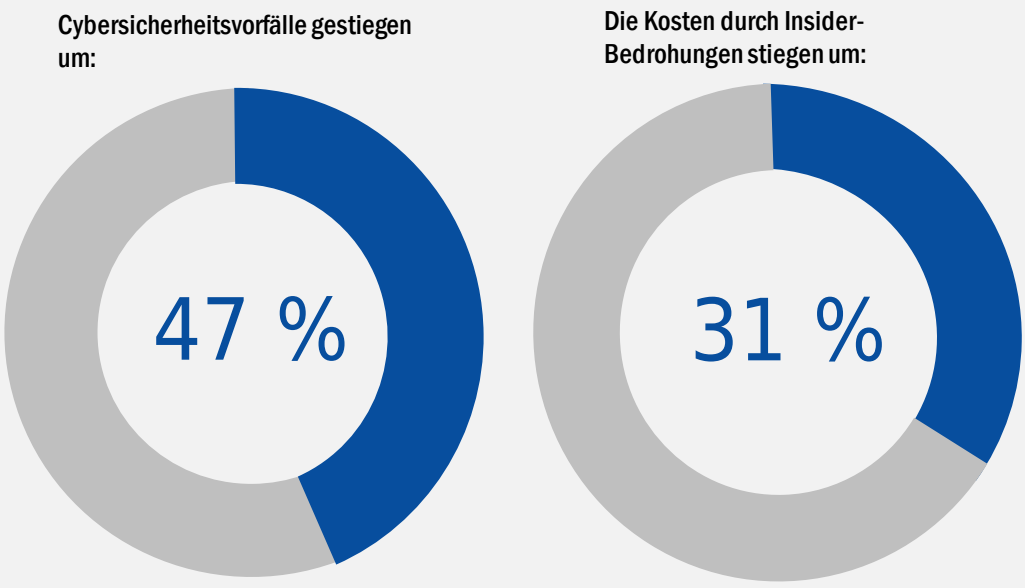


Abbildung 2: Vorfälle und Kostentrends Quelle: ObservelT[8]

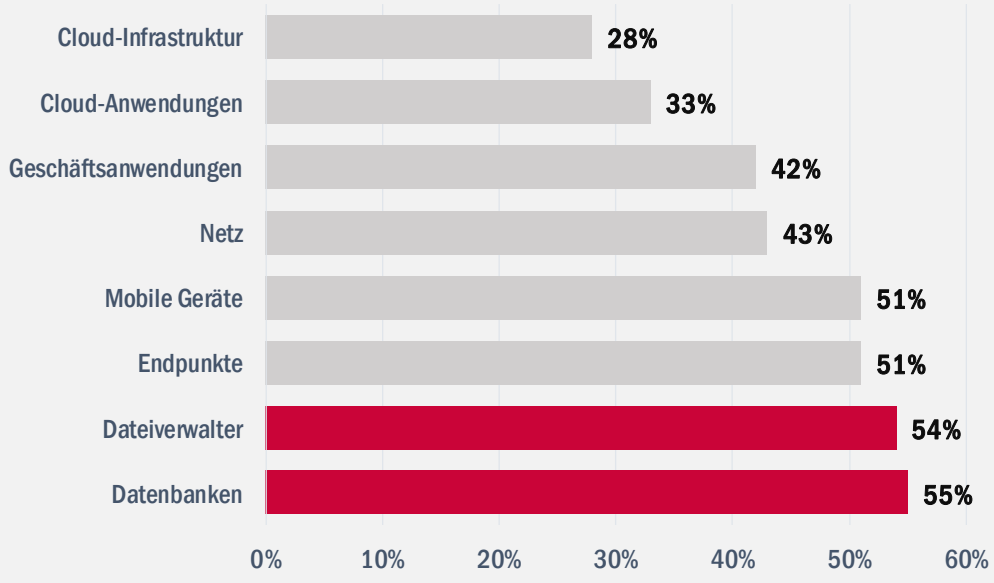


Abbildung 2: IT-Ressourcen sind anfällig für Insiderbedrohungen. Quelle: Help Systems[9]

Angriffsvektoren

_Wie

Eine kürzlich durchgeführte Umfrage[14] ergab, dass Gruppen die gefährlichsten Insider-Bedrohungen in Unternehmen und anderen Organisationen darstellen.

Laut Cybersicherheitsexperten[15], ist Phishing (38 %) die größte Sicherheitslücke bei unbeabsichtigten Insider-Bedrohungen. Weiter unten auf der Liste stehen Spear Phishing (21 %), schwache oder wiederverwendete Passwörter (16 %), verwaiste Konten (10 %) und das Durchsuchen verdächtiger Websites (7 %).

_ Wirkungsbereich von Insiderbedrohungsvorfällen

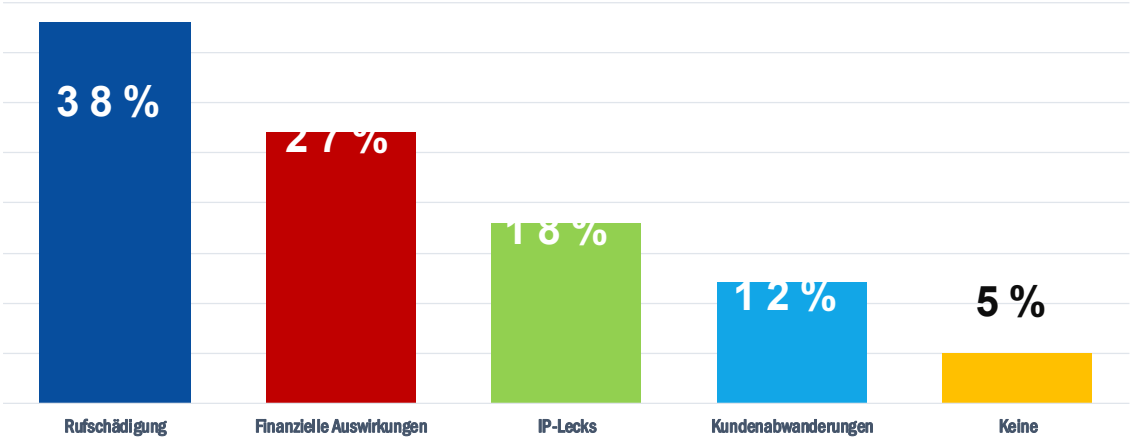


Abbildung 3 - Quelle: Egress[12]


„Insider können unbeabsichtigt durch Nachlässigkeit oder mangelndes Wissen Schaden anrichten.“
In ETL 2020

Minderung

Vorgeschlagene Maßnahmen

- Stellen Sie eine Deep Packet Inspection (DPI) -Technologie zur Erkennung von Anomalien bereit, die industriellen Benutzern eine vertrauenswürdige Plattform zur Überwachung des Ablaufs von Befehlsfluss- und Telemetriedaten zur Prozesssteuerung und zum Schutz vor externen Bedrohungen bietet. Gleichzeitig wird das Risiko „fortgeschrittener" Insider-Eingriffe von Technikern, SCADA-Betreibern oder anderen internen Mitarbeitern mit direktem Zugriff auf Systeme verringert.[16]
- Führen Sie einen Plan für Gegenmaßnahmen gegen Insider-Bedrohungen in die allgemeine Sicherheitsstrategie und -richtlinien ein. Dieser Plan umfasst in der Regel ein Risikomanagement-Framework, einen Business Continuity Plan (BCP), ein Disaster Recovery-Programm (DRP), Richtlinien für das Finanz- und Rechnungswesen sowie ein finanzielles und regulatorisches Management.[1]
- Erstellen Sie ein Sicherheitsprogramm, das Folgendes umfasst: Durchführen von Aktivitäten zur Bedrohungssuche, Durchführen von Schwachstellen-Scans und Penetrationstests, Implementieren von Sicherheitsmaßnahmen für das Personal, Einsatz physischer Sicherheitsmaßnahmen, Implementierung von Netzwerksicherheitslösungen, Einsatz von Endpunkt-Sicherheitslösungen, Anwendung von Datensicherheitsmaßnahmen, Einsatz von Identitätsicherungs- und Zugriffsmanagementmaßnahmen, Einrichtung von Incident Management-Funktionen, Beibehaltung digitaler Forensikdienste und Einsatz künstlicher Intelligenz (KI) zur Verhinderung von Insiderangriffen.
- Erstellung einer Sicherheitsrichtlinie für Insiderbedrohungen, basierend auf dem Bewusstsein der Benutzer, die eine der effektivsten Kontrollen für diese Art von Cyberbedrohungen darstellt.
- Implementierung robuster technischer Kontrollen. Herkömmliche Sicherheitsmaßnahmen konzentrieren sich in der Regel auf externe Bedrohungen, aber diese sind normalerweise nicht effizient bei der Identifizierung interner Risiken, die von innerhalb des Unternehmens ausgehen. Implementierung von Instrumenten zum Schutz von Ressourcen, wie z.B. DLP (Data Loss Prevention), um die Datenexfiltration zu verhindern.[1]

- Reduzierung der Anzahl der Benutzer mit Berechtigungen und Zugriff auf vertrauliche Informationen. Wenn ein Mitarbeiter für seine Arbeit keinen Zugriff auf bestimmte Informationen haben muss, ist es besser, die Sichtbarkeit einzuschränken, um einen unzulässigen Zugriff zu vermeiden.[17]
- Abhärtung der digitalen Umgebung, einschließlich der Verbesserung der Sicherheit des Netzwerks, der Systeme, Anwendungen, Daten und Konten.[1]

Literaturangaben

1. "Insider Threat Report", 2019. Verizon. https://enterprise.verizon.com/resources/reports/insider-threat-report.pdf

2. "Insider Threat Statistics Facts and Figures". Ekran System. https://www.ekransystem.com/en/blog/insider-threat-statistics-facts-and-figures

3. "CyberEdge 2019 CDR Report" 2019. CyberEdge. https://cyber-edge.com/wp-content/uploads/2019/03/CyberEdge-2019-CDR-Report.pdf

4. "Corporate Security Predictions 2020". 2019. 3. Dezember, 2019. Kapersky.

https://securelist.com/corporate-security-predictions-2020/95387/

5. "Famous Insider Threat Cases" September 2019. Security Boulevard. https://securityboulevard.com/2019/09/famous-insider-threat-cases-insider-threat-awareness-month/

6 "The rise of insider threats: Key trends to watch" 2019. Tech Beacon.

https://techbeacon.com/security/rise-insider-threats-key-trends-watch

7. "Cost of Cybercrime study" 2019. Accenture. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

8. "Cost of Insider Threats", 2020. Observer IT. https://www.observeit.com/cost-of-insider-threats/

9. "Cybersecurity Insiders 2019 Insider Threat Report", 2019. Help Systems.https://www.helpsystems.com/cta/2019-cybersecurity-insiders-insider-threat-report

10. "Forcepoint Insider threat Data Protection" 2017. Force Point.

https://www.forcepoint.com/sites/default/files/resources/files/brochure_insider_threat_data_protection_en.pdf

11. "State of Insider Threats in the Digital Workplace" 2019. Better Cloud. https://www.bettercloud.com/monitor/wp-content/uploads/sites/3/2019/03/BetterCloud-State-of-Insider-Threats-2019-FINAL.pdf

12. "Insider Data Breach Survey 2019". 2019. Egress. https://scoop-cms.s3.amazonaws.com/566e8c75ca2f3a5d5d8b45ae/documents/egress-opinionmatters-insider-threat-research-report-a4-uk-digital.pdf

13. "Insider Threat Report". 2019. Nucleos Cyber. https://nucleuscyber.com/wp-content/uploads/2019/07/2019_Insider-Threat-Report_Nucleus_Final.pdf

14. "Insider Threat Report". 2019. Haystax. https://haystax.com/wp-content/uploads/2019/07/Haystax-Insider-Threat-Report-2019.pdf

15. "Insider Threat Report". 2019. Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/insider-threat-report.pdf

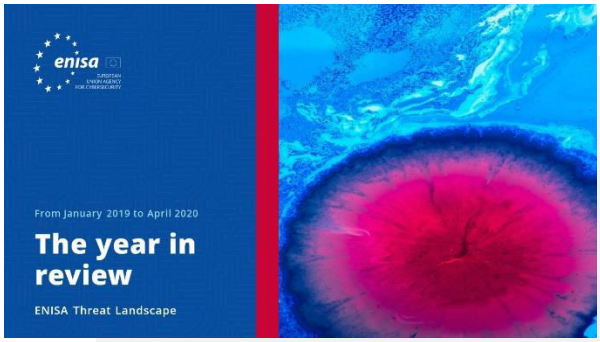
16. "Kaspersky Industrial CyberSecurity: solution overview 2019". 2019. Kaspersky. https://ics.kaspersky.com/media/KICS-Solution-overview-2019-EN.pdf

17. "Post-vacation cybersecurity tuneup: Get your company ready!". 1. September, 2017. Panda. https://www.pandasecurity.com/mediacenter/adaptive-defense/cyber-security-get-company-ready/

Die zunehmende Komplexität von Webanwendungen und ihren weit verbreiteten Diensten schafft Herausforderungen bei der Sicherung derselben gegen Bedrohungen mit unterschiedlichen Motiven, von finanziellen oder Reputationsschäden bis hin zum Diebstahl kritischer oder personenbezogener Daten. “

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**

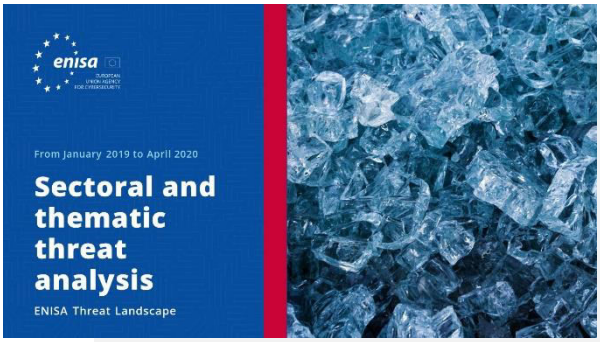
ENISAs-Liste der 15 größten Bedrohungen im Zeitraum zwischen Januar 2019 und April 2020.

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