Microsoft Security

Cybercrime: Attacken im Minutentakt

Die Bekämpfung von Cyberkriminalität ist eine große Herausforderung – und sie wird größer: Die Bedrohungslandschaft entwickelt sich stetig weiter und umfasst immer mehr Geräte, Umgebungen und Szenarien. Dass bei einem Cyberangriff jede Sekunde zählt, wird umso deutlicher, wenn wir das Ausmaß der weltweiten Cyberkriminalität von Minute zu Minute betrachten. Um dies zu veranschaulichen, haben wir die Angriffe innerhalb eines Jahres anhand unserer Forschungsergebnisse in 60-Sekunden-Fenstern aufgeschlüsselt.

Die Bedrohungslandschaft von heute

In jedem beliebigen 60-Sekunden-Fenster jeder Stunde eines Tages sind Hacker*innen aktiv:

Angriffe auf Passwörter	34.740 pro Minute [1]
IoT-basierte Attacken	1.902 pro Minute [2]
DDoS-Attacken	1.095 pro Minute [3]
Phishing-Angriffe	7 pro Minute [4]
SQL-Injection-Attacken	1 alle 2 Minuten [5]
Entdecken neuer Infrastrukturen, die IT-Systeme bedrohen	1 alle 35 Minuten [6]
Angriffe auf Lieferketten	1 alle 44 Minuten [7]
Ransomware-Attacken	1 alle 195 Minuten [8]

* Die Zahlen stammen aus Daten von RiskIQ, einem führenden Unternehmen im Bereich der globalen Bedrohungsanalyse. RiskIQ gehört seit 2021 zu Microsoft und unterstützt seine Kunden dabei, die Sicherheit ihrer gesamten digitalen Infrastruktur zu bewerten.

Daten von Microsoft

Über die globalen Dienste, die Microsoft in großem Umfang betreibt, können wir Bedrohungssignale aus der ganzen Welt und aus einer Vielzahl von Branchen identifizieren, aggregieren und korrelieren. Unsere Sicherheitsforscher*innen analysieren das vielfältige Spektrum an Daten von Endpunkten, Identitäten, Anwendungen und aus der Cloud, um ein genaues Bild der aktuellen Bedrohungslandschaft zu erhalten.

18.265
Malware-Bedrohungen (die der Microsoft Defender for Endpoint blockiert)
pro Minute [9]

48.706
Brute-Force-Attacken auf Authentifizierungs-Dienste (von Azure Active Directory blockiert)
pro Minute [10]

133.181
Angriffe (verhindert durch Microsoft)
pro Minute [11]

58.980
Bedrohungen von Identitäten (blockiert von Microsoft)
pro Minute [12]

17.123
Bedrohungen von Endpunkten (blockiert von Microsoft)
pro Minute [13]

60.882
Bedrohungen über E-Mails (blockiert von Microsoft)
pro Minute [14]

1.065
Von Microsoft entdeckte offene Ports
pro Minute [15]

Das kostet uns Cyberkriminalität

Cyberkriminalität verursacht hohe volks- und betriebswirtschaftliche Schäden, die Unternehmen in ihrer Existenz bedrohen können. Der Branchenverband Bitkom schätzt, dass durch Diebstahl, Spionage und Sabotage der deutschen Wirtschaft jährlich ein Gesamtschaden von 223 Milliarden Euro entsteht – und damit mehr als doppelt so viel wie in den Jahren 2018/2019. Die Kosten der Cyberkriminalität ergeben sich aus den unmittelbaren Schäden an IT-Infrastrukturen, aus dem Diebstahl von Vermögenswerten – einschließlich geistigen Eigentums – und der Unterbrechung regulärer Geschäftstätigkeiten.

1.151.339 €
Wirtschaftliche Auswirkungen von Cyberkriminalität
pro Minute [18]

287.835 €
Ausgaben für Cybersicherheit
pro Minute [19]

38.378 €
Verluste durch Betrug im E-Commerce-Zahlungsverkehr
pro Minute [20]

38.377 €
Schaden durch Ransomware
pro Minute [21]

3.646 €
Betrag, der durch Betrug mit Kryptowährungen verloren ging
pro Minute [22]

4.631 €
Gesamtkosten von Kompromittierungen über Business-E-Mails
pro Minute [23]

8 €
Durchschnittliche Kosten eines Einbruchs in eine IT-Infrastruktur
pro Minute [24]

5 €
Durchschnittliche Kosten eines Malware-Angriffs
pro Minute [25]

Bedrohungslage in Internet und Cloud

Mit der wachsenden Verbreitung des Internets mehren sich auch hier die Angriffsmöglichkeiten für Hacker*innen. Besonders im Fokus stehen Unternehmen, die ihre Infrastrukturen zunehmend in die Cloud migrieren und dort innovative Projekte starten. Zudem setzen immer mehr Mitarbeiter*innen in einer zunehmend hybriden Arbeitswelt eigene Geräte ein („Schatten-IT"), die von den Unternehmen über das Internet in firmeneigene Netze integriert und über die Cloud administriert werden. Daraus entstehen komplexe, oft über mehrere Clouds verteilte IT-Systeme – und damit zunehmend komplexe und unübersichtliche Angriffsvektoren für Cyberkriminelle.

Neue Hosts	79.861 pro Minute [26]
Neue IoT-Geräte	7.620 pro Minute [27]
Neue Domains	150 pro Minute [28]
Neue aktive Lets-Encrypt SSL-Zertifikate	53 pro Minute [29]
Neue mobile Apps	23 pro Minute [30]

Fazit

Die weltweite Bedrohungslandschaft durch Cyberkriminalität entwickelt sich äußerst dynamisch. Microsoft analysiert über seine Anwendungen und Systeme täglich mehr als 24 Billionen Signale, um diese Landschaft zu analysieren und auf akute, wie neuartige Bedrohungen umgehend reagieren zu können. Wir stellen diese Informationen und unsere Tools auch unseren Partnern und Kunden zur Verfügung, damit auch sie reagieren können und handlungsfähig bleiben.

Quellen

1 https://www.microsoft.com/security/blog/2021/05/12/securing-a-new-world-of-hybrid-work-what-to-know-and-what-to-do/
2 https://www.netscout.com/threatreport
3 https://www.itechpost.com/articles/110312/20220426/crime-grows-technology-1-billion-iot-devices-suffered-attacks-2021.htm#:~:text=In%202021%2C%20there%20was%20more,of%20cyberattacks%20to%20be%20successful
4 https://www.helpnetsecurity.com/2022/03/03/phishing-attacks-december-2021
5 https://owasp.org/Top10/A03_2021-Injection/
6 RiskIQ detection
7 https://www.sonatype.com/resources/state-of-the-software-supply-chain-2021
8 https://www.securitymagazine.com/articles/97166-ransomware-attacks-nearly-doubled-in-2021
9 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWUGFg
10 https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWUGFg
11 https://www.microsoft.com/en-us/Investor/earnings/FY-2022-Q1/press-release-webcast
12 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
13 https://www.microsoft.com/en-us/Investor/earnings/FY-2022-Q1/press-release-webcast
14 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
15 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
16 https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
17 RiskIQ detections
18 https://www.csis.org/analysis/economic-impact-cybercrime
19 https://www.dataprise.com/resources/blog/2022-cybersecurity-spending
20 https://www.statista.com/statistics/1273177/ecommerce-payment-fraud-losses-globally
21 https://www.cybereason.com/hubfs/dam/collateral/ebooks/Cybereason_Ransomware_Research_2021.pdf
22 https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/
23 https://news.microsoft.com/on-the-issues/2022/05/03/how-microsofts-digital-crimes-unit-fights-cybercrime/
24 https://apps.preview.powerapps.com/play/e/839eace6-59ab-4243-97ec-a5b8fcc104e4/a/c8224e96-5247-41e9-8c72-af63d291564f?tenantId=72f988bf-86f1-41af-91ab-2d7cd011db47
25 https://cobalt.io/blog/business-cost-of-cybercrime
26 RiskIQ detections
27 https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2
28 RiskIQ detection
29 https://letsencrypt.org/stats/#growth
30 Evil Internet Minute infographic. Requires update