Wie gelingt der nächste Quantensprung im Schwachstellen- und Bedrohungsmanagement?

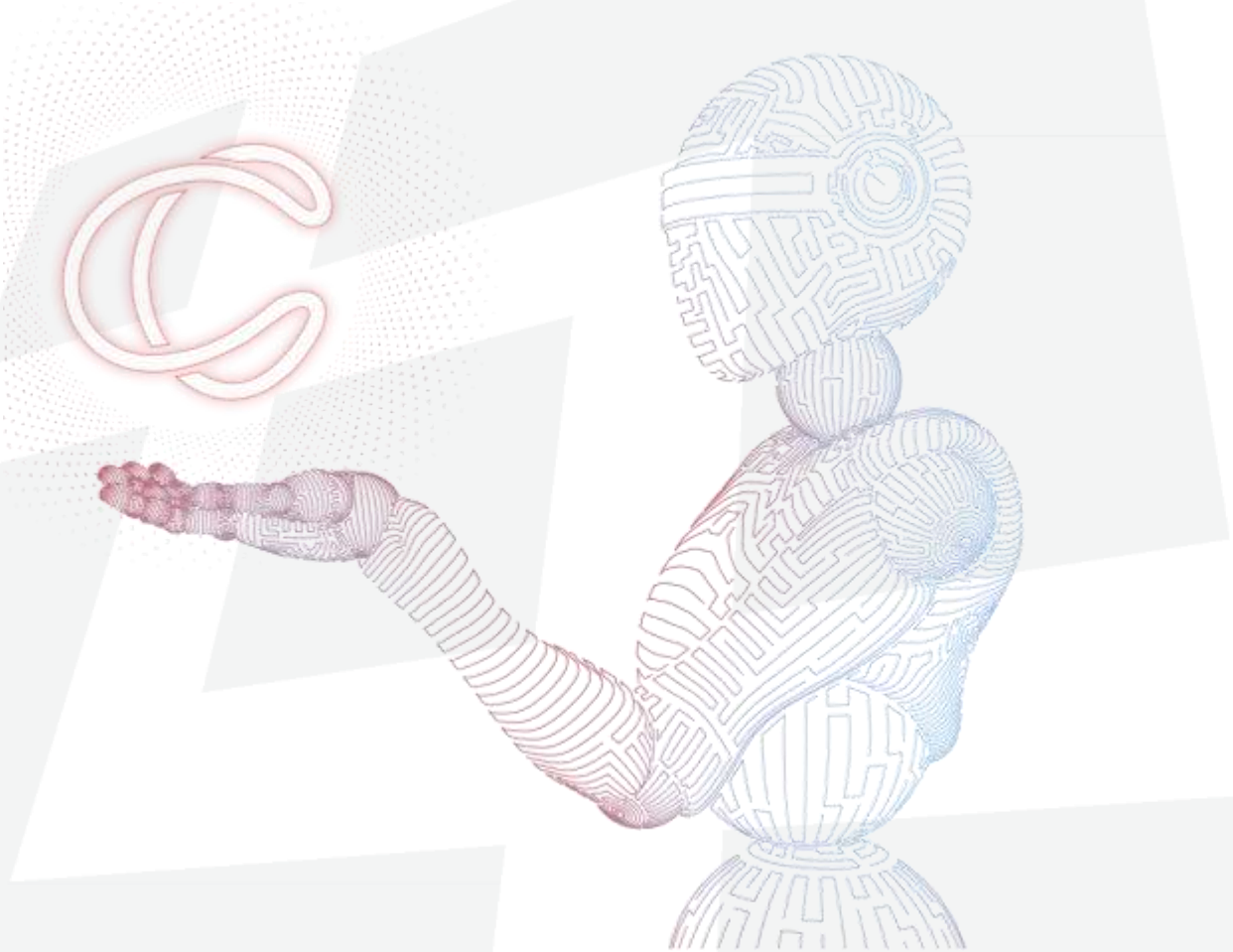
DEUTSCHE GESELLSCHAFT FÜR
CYBERSICHERHEIT

Bedrohungslage und Lösungsansätze

Einführung

Die aktuelle Cybersicherheitslandschaft entwickelt sich rasant zu einer überwältigenden Bedrohungsfläche für Unternehmen und den öffentlichen Sektor.

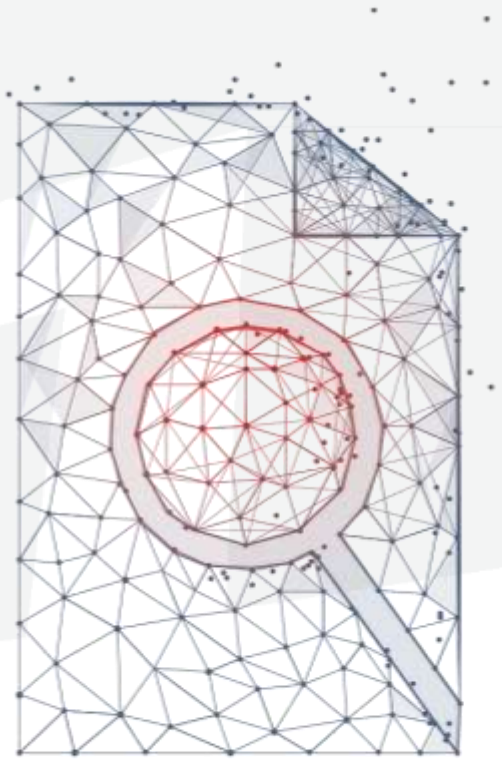
Innovative Lösungen zur wesentlichen Verbesserung des Schwachstellen- und Bedrohungsmanagement sind erforderlich, um mit der sich stetig multiplizierenden Bedrohungslage, Schritt zu halten. Wir betrachten neuartige ganzheitliche Ansätze zur effizienten Sicherung von IT-Assets jeglicher Art.



Bedrohungslage 2022

Fakten & Zahlen

- Kontinuierlich wachsender Trend bei neu entdeckter Malware (153 Millionen) mit über 90 % polymorphem Code.
- Verwendung von ECC- statt RSA-Verschlüsselung durch deutlich höheren Verschlüsselungsfaktor bei geringerer Schlüssellänge (256 vs. 3072).
- 75 % der Malware wird über E-Mail- und Phishing-Kampagnen eingeschleust.
- Die Zusammenarbeit von Organisationen der Cyberkriminalität wird fortgesetzt und wächst (Trickbot setzt Emotet ein, um den Angriff erneut zu aktivieren)
- Angriffe auf die Supply-Chain (z. B. APT27 LuckyMouse, das auf Pharma- und Technologie-KMU abzielt, REvil-Angriff auf Quanta Computer, um Apple MacBook Pro-Designs zu erhalten usw.).
- Deepfake & Voice-Phishing, um Identitäten zu imitieren (d.h. HK Back 35$M).



Bedrohungslage 2022

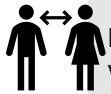
Kosten vs. Cybersecurity Readiness

- 50 % Prozent aller kompromittierten Unternehmen akzeptieren Lösegeldzahlungen.
- Durchschnittlich 12 % des gesamten IT-Budgets werden in den Sicherheitsbereich investiert.
- Die durchschnittlichen wirtschaftlichen Auswirkungen pro Vorfall liegen zwischen 1,73 Mio. € und 3,7 Mio. €.
- ~20 % der Unternehmen haben automatisierte Sicherheitsmaßnahmen implementiert.
- Durchschnittliche Breach-Detection von 207 Tagen, gefolgt von 73 Tagen, um den Betrieb erfolgreich wiederherzustellen und / oder zu isolieren.

WIE HACKER IN SYSTEME EINDRINGEN

Man-In-The-Middle (MitM)

Bei diesem Angriff platziert sich der Angreifer zwischen den beiden Kommunikationspartnern (zwischen Opfer und den verwendeten Ressourcen).



Social Engineering Angriff

Bei Social Engineering Angriffen werden Phishing E-Mails durch manipulative Informationsbeschaffung genau auf ihre beabsichtigten Opfer zugeschnitten.

(Brute Force) Passwort Angriffe

Cyberkriminelle nutzen Mechanismen zur Authentifizierung von Passwörtern, um Zugang zu Nutzerdaten zu erlangen.

Cryptojacking

Beim Cryptojacking schürfen Cyberkriminelle unbemerkt Kryptowährung über den Browser fremder Computer oder Geräte.

Phishing & Spearphishing

Bei dieser Art von Cyberangriff werden betrügerische E-Mails versendet, die Schadcode in Form von Verlinkungen enthalten.

SQL-Injection-Attacke

Angreifer nutzen eine häufig durch Programmierfehler entstandene Sicherheitslücke aus, die in Zusammenhang mit einer SQL-Datenbank steht.

Denial of Service (DoS)

Bei einem Denial of Service Angriff, machen die Angreifer einen Server unzugänglich und setzen ihn gezielt außer Betrieb.

Abhörangriffe (Eavesdropping)

Bei dieser Art von Angriff fangen Hacker Daten ab, die zwischen zwei Geräten übertragen werden und belauschen Gespräche sowie Netzwerkaktivitäten.

Drive-By Angriff

In Drive-By Angriffen verwenden Hacker unsichere Webseiten, um darüber Malware zu verbreiten.

Malware-Angriff

Malware ist jegliche Software, die ohne Zustimmung des Opfers, unerwünschte und schädliche Funktionen auf dem Computer ausführt.

Distributed Denial of Service (DDoS)

Hier kommt eine hohe Anzahl von gleichzeitig angreifenden Systemen zum Einsatz, um großflächig Server außer Betrieb zu setzen.

Botnet Attacke

Ein Botnet ist eine Gruppe infizierter Computer mit automatisierter Schadsoftware, die als Netzwerk zusammenarbeitet.

Cross-Site Scripting (XSS)

Bei dieser Art von Cyberangriff wird eine Webseite mithilfe einer Sicherheitslücke ausgenutzt, um bösartigen Code in einen vermeintlich sicheren Kontext einzubetten.

Innerer Angriff

Diese Art von Attacke erfolgt aus dem Inneren der eigenen Systeme, z.B. durch ehemalige oder verärgerte Mitarbeiter*innen, und ist daher besonders gefährlich.

Wie gelingt der nächste Quantensprung?

WISSEN IST MACHT .....

cyberscan.io ®

Das IT-Security Tool der nächsten Generation

cyberscan.io® ist ein auf Sicherheitsmaßnahmen ausgelegtes Portal, das Funktionen von Schwachstellenscanner, Penetrationswerkzeug und Open Source Intelligence-Tool kombiniert.

Sämtliche IP-Adressen und Sub-Domains einer Domain werden identifiziert und nach Schwachstellen durchsucht. Nach dem Scannen Ihrer Informationen erfolgt der Abgleich mit einer Vielzahl seriöser Quellen zur Bedrohungsanalyse. Die Ergebnisse werden samt Risikoeinstufung übersichtlich in unserem Dashboard dargestellt und können zur Weiterverarbeitung in Reportform archiviert werden.

cyberscan.io

Features in der Übersicht

Incident Alert Engine

Automatisierte Benachrichtigung über neue Schwachstellen und Sicherheitsrisiken.

Management Portal

Ein übersichtliches All-in-One Dashboard, mit dem Sie alle Ihre Domains und IP-Adressen im Blick behalten.

Automatisches Reporting

Automatisierte und übersichtliche Dokumentation sämtlicher Kennzahlen aus cyberscan.io®.

Datenleck Monitoring

Mehr als 15 Millionen Datenlecks/Data Breaches in einer integrierten Datenbank zur Überprüfung der eigenen Firmen-E-Mail-Accounts.

Real Time Internet Monitoring

Kontinuierliches Scannen und Konsolidieren von mehr als 130 Internet-Quellen (darunter Shodan).

Netzwerke & Organisation

Übersicht über die Anzahl der Schwachstellen innerhalb der Netzwerke, zu denen Ihr Server gehört.

Big Data Repository

Mehr als 7 Millionen Bulletins in unserer selbstlernenden Datenbank – darunter 160.000 Schwachstellen, die in der Liste öffentlicher Schwachstellen und Risiken (CVE) geführt sind.

Artificial Intelligence

KI-basierte Analyse der Schwachstellen und Mapping in unserer Datenbank.

CISCO & DGC

Eine starke Partnerschaft

Die Deutsche Gesellschaft für Cybersicherheit (DGC) bündelt ihre Kompetenzen als führender Anbieter für Cyber Security und Datenschutz mit dem Know-how von Cisco, dem Marktführer für Netzwerksicherheit. Die beiden IT-Dienstleister verbünden sich im Kampf gegen Bedrohungen aus dem Netz und schaffen für ihre Kunden ganzheitlichen IT-Schutz.

Im Zentrum der Partnerschaft stehen mit den Produkten **cyberscan.io®** im Bereich Schwachstellenerkennung sowie der Extended Detection & Response Plattform (**SecureX**) zwei Tools, die zusammen einen umfassenden Schutz vor verschiedensten Bedrohungen bieten

Mit der gegenseitigen Tool-Integration können Unternehmen ihre IT-Systemlandschaft kontinuierlich überwachen und Sicherheitslücken reaktionsschnell schließen.

Vielen Dank für die Aufmerksamkeit!

DEUTSCHE GESELLSCHAFT FÜR CYBERSICHERHEIT mbH & Co. KG

Am Fördeufer 1b
DE-24944 Flensburg

Tel: +49 461 995 838 0

info@dgc.org
www.dgc.org

Folgen Sie uns in den sozialen Medien, um täglich Beiträge zu den neusten Schwachstellen, Datenpannen und IT- Sicherheitsnews zu erhalten!

bitkom Cyber-Sicherheitsrat Deutschland e.V. SecurITy Allianz für Cyber-Sicherheit Partner