glueckkanja

glueckkanja
Patrick Boeck

Die neue Realität der Cyberangriffe: Effizient, zielgerichtet, KI-getrieben

glueckkanja

Zero Day Clock: Die Zeit zum Exploit kollabiert

2019

702

Tage Median

Von CVE-Offenlegung bis zum ersten beobachteten Exploit

2021

84

Tage Median

9-fache Kompression in drei Jahren – Log4Shell binnen Stunden ausgenutzt

2024

6,36

Tage Median

44 % der Exploits innerhalb von 24 h – 40 % sind Zero-Days

2026

10

Stunden Ø

Exploits erscheinen jetzt am selben Arbeitstag wie die Offenlegung

Von 702 Tagen auf 10 Stunden in sieben Jahren. Der 30-Tage-Patchzyklus ist ein Relikt.

Quelle: zerodayclock.com – 83.000+ CVEs aus CISA KEV, ExploitDB, Metasploit

glueckkanja

Warum es jetzt kippt: AI weaponisiert Patches

> **Jeder Patch ist ein Exploit-Blueprint.**
> AI verkürzt die Zeit, den Blueprint in einen funktionierenden Exploit zu verwandeln, dramatisch.
> *— Signatories, Zero Day Clock*

80 % der Exploits vor dem Advisory

Im Schnitt 23 Tage, bevor die offizielle Warnung erscheint. Das Disclosure-System ist invertiert: Es warnt Verteidiger nach dem Angriff.

Scoring wird zur Post-Mortem-Übung

CVSS und Priorisierungs-Frameworks setzen Zeit voraus, die Verteidiger haben. Bei Minuten-Exploitation ist das Ranking zu spät.

Kalender gegen Stoppuhr

30-Tage-Patchzyklen treffen auf eine mittlere Time-to-Exploit von unter zwei Tagen. Wer mit dem Kalender zum Uhrenkampf kommt, endet im Post-Mortem statt mit Lessons Learned.

glueckkanja

Was jetzt zählt: Von Kalender zu Clock-Speed

Secure-by-Default

Architektonische Mitigations, die standardmäßig aktiv sind – nicht als Opt-in. Nur Schutz, der schon läuft, greift in Stunden.

DIE statt CIA

Distributed, Immutable, Ephemeral: Systeme, die Minuten leben, bieten Angreifern nichts zum Stehlen und nichts zum Verstecken.

Bug-Klassen eliminieren

Rund 70 % kritischer Bugs sind Memory-Safety-Fehler. Rust & Co. machen sie strukturell unmöglich – nicht nur seltener.

Speed als KPI

MTTR in Stunden statt Tagen. Erfolg misst sich nicht in Patch-Compliance, sondern in der gelebten Geschwindigkeit zwischen Erkennen und Wirken.

Die Frage ist nicht mehr „sind wir compliant?“ – sondern „sind wir schnell genug?“

glueckkanja

Phishing: Unverändert der Angriffsvektor Nr. 1

WARUM ES WEITER FUNKTIONIERT

Ein Überzeugter Klick schlägt jede Firewall.

Phishing bleibt der effizienteste Angriffsvektor unserer Zeit: niedrige Kosten, hohe Skalierung, direkter Zugriff auf Identitäten und Zahlungsflüsse – und der Mensch als Ziel, nicht die Technik.

Die Professionalisierung ist spürbar

Kontextbezogener Köder

Angreifer referenzieren reale Vorgänge – aus Leaks, LinkedIn oder Supply-Chain-Kompromittierungen. Die Mail wirkt nicht erfunden, sondern anschlussfähig.

KI-generierte Formulierung

Keine Rechtschreibfehler, kein gebrochenes Deutsch. Tonalität und Branding werden perfekt imitiert – auf jeder Sprache.

Industrialisiert: Phishing-as-a-Service

Fertige Kits, Landing-Pages und Support-Hotlines für Angreifer. Der Einstieg kostet weniger als eine Office-Lizenz.

glueckkanja

Vishing: Wenn die Stimme am Telefon gefälscht ist

ERSTE REALE FÄLLE BEI UNS

Stimme klonen – geht in Sekunden.

Mit wenigen Sekunden Audiomaterial – aus Konferenzvideos, Podcasts, Voice-Mails – lässt sich die Stimme einer Kollegin oder Führungskraft synthetisieren oder live synchronisieren. Anruf ≠ Identitätsnachweis.

Gemeldete Angriffsmuster

Erzwungener Passwort-Reset

„Hier ist Max aus der Geschäftsleitung, ich sitze im Ausland fest – brauche sofort einen Reset.“ Der Druck ist echt, die Stimme auch. Nur die Person nicht.

CEO-Fraud 2.0

Anweisung zur Eilüberweisung oder Freigabe per Anruf mit gekloneter Chefstimme – kombiniert mit einer Phishing-Mail, die den Anruf „ankündigt“.

Help-Desk-Manipulation

Der vermeintliche Mitarbeiter ruft IT-Support an und erzwingt MFA-Reset oder Geräteregistrierung. Die Identitätsprüfung basiert oft nur auf „Ich klinge wie er“.

Kombi mit Echtzeit-Synchronisierung

Live-Voice-Conversion während des Gesprächs: Der Angreifer spricht natürlich, das Opfer hört die Zielstimme. Akzent, Dialekt, Tonalität – alles passend.

glueckkanja

Video-Deepfake: Wenn das Teams-Meeting lügt

Mit frei verfügbaren Tools lässt sich heute aus einem einzigen Porträtfoto ein sprechender Avatar erzeugen – live im Videocall, mit synchronisierten Lippenbewegungen. Das folgende Beispiel zeigt, wie nah wir bereits am Alltag sind:

Patrick Böck

Sandro Bachmann

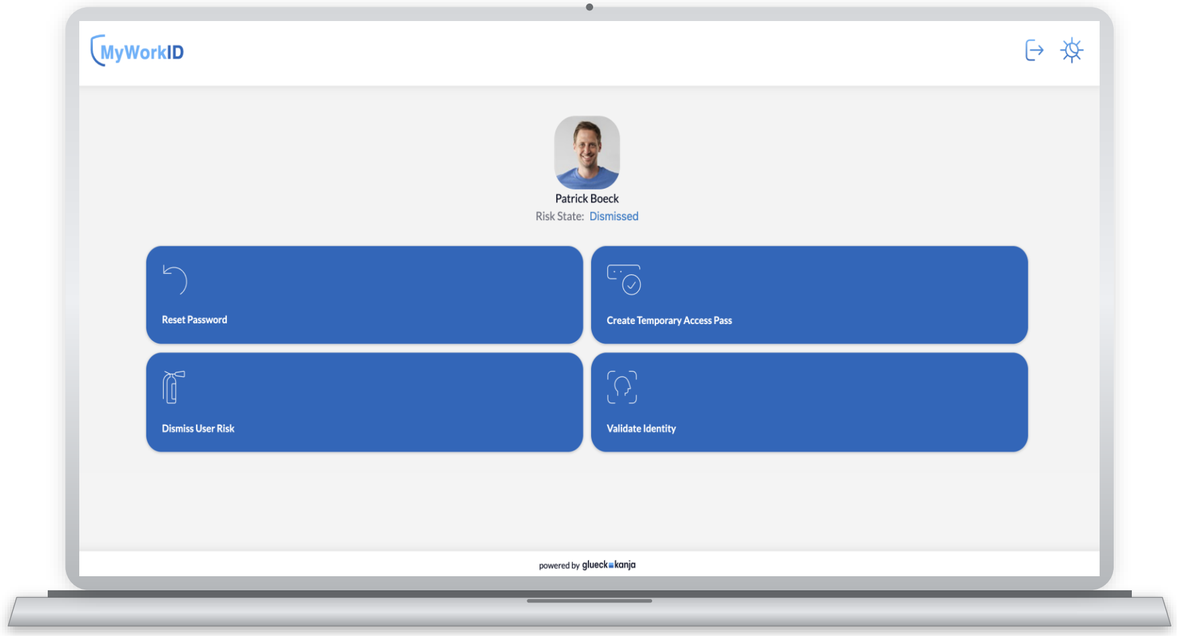
Stefan Läufle

Konsequenz: Identität muss belegt werden – nicht geglaubt. Zweiter Kanal, Code-Wort, verifiziertes Gerät.

Live-Demo: Drei Avatare in Aktion

glueckkanja

Unsere Antwort: MyWorkID – Identität belegen, nicht glauben



UNSERE LÖSUNG

Help-Desk bekommt einen verlässlichen zweiten Kanal.

Verified ID – Identitätsnachweis kryptographisch

Der Mitarbeiter weist sich über Microsoft Entra Verified ID aus. Keine Rückfrage am Telefon, kein Bauchgefühl – ein kryptographisch signierter Credential statt einer geklonten Stimme.

Face-Match gegen Entra-Profilfoto

Live-Selfie wird gegen das hinterlegte Profilbild in Entra geprüft. Der Admin sieht einen Matching-Score in Prozent – Deepfake- und Stand-in-Versuche fallen durch den Vergleich auf.

Kontrollierte Admin-Aktionen

Erst nach erfolgreicher Verifikation: Reset Password, Temporary Access Pass, Dismiss User Risk oder Validate Identity – zentral, auditierbar, ohne Umweg über den IT-Support am Telefon.

Aus „Ich glaube dir“ wird „Ich verifiziere dich“ – in unter einer Minute.

→ MEHR ERFAHREN
glueckkanja.com/en/security/my-work-id

glueckkanja

Assume Breach: Nicht ob, sondern wann

**„Die Frage ist nicht, ob Sie angegriffen werden –
sondern wann und wie gut Sie vorbereitet sind.“**

GESTERN

Nur Prevent

Firewalls, Passwörter, Schulungen.
Annahme: Wir halten sie draußen.

HEUTE

Detect & Respond

SOC, EDR, 24/7-Monitoring. Annahme:
Sie sind schon drin – finde sie.

MORGEN

Assume Breach

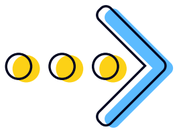
Vorbereitung auf den Ernstfall. Wenn
Identität und Systeme fallen:
Wiederaufbau in Stunden.

Resilienz misst sich nicht an der Höhe der Mauer – sondern an der Geschwindigkeit des Wiederaufbaus.

glueck kanja

Aus der Praxis – Probleme im Ernstfall

Digitale Kommunikation ist tot

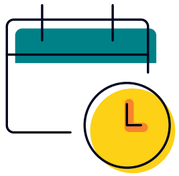


Identitäten sind Ausgangspunkt für Restore – Domain Controller ist die Basis der meisten (Legacy-) Anwendungen

Kein Vertrauen mehr in die bestehende Infrastruktur

Externe Parteien verzögern den Restore

Greenfield für AD-Domain fast unmöglich



Prozesse fehlen – die Zeit läuft davon

glueck kanja

Ziele des Managed Dark Tenant

Lösung, die kritische Services schützt und einem erfolgreichen Ransomware-Angriff standhält.

Kritische Services bestehen aus:

Active Directory

Identitäten

Kritische Dokumente und Daten

Optional: Kritische Geschäftsanwendungen

Automatisierter Prozess für eine Kollaborationsplattform für ausgewählte Nutzer in den ersten Stunden nach dem Angriff.

Skalierbare und gesicherte Virtual Desktop Infrastructure

RTO für kritischste Dienste: wenige Stunden nach dem Angriff

Starker Fokus auf REGELMÄSSIGE Fire-Drills

100 % DevOps – Infrastructure as Code mit Terraform

glueck kanja

We Manage and Protect Microsoft Ecosystems at Scale

Workplace | Security | Azure | Companion Products