Aussteller-Presseevent: Eye Security GmbH

Breakfast before Breaches mit Chief Hacker Vaisha Bernard.

Wie Hacker heute vorgehen:
aktuelle Angriffsmethoden, Sicherheitslücken und neue Entwicklungen bei Cyberangriffen.



Über eine kurze Anmeldung vorab bei Antje Schäfer unter antje.schaefer@eye.security freuen wir uns.

Datum: Mittwoch, 28. Oktober 2026
Uhrzeit: 10:00 Uhr
Ort: Halle 8, Stand 8-209

Alle Pressematerialien zur it-sa 2026

Hier finden Sie alle Materialien zur it-sa 2026 zum Download:
Unser Logo, die Unternehmenspräsentation, Pressemitteilungen, den Innovations-Newsletter und die Einladung zum Presse-Frühstück.

© 2026 Eye Security. Alle Rechte vorbehalten. Die in dieser Veröffentlichung enthaltenen Informationen dienen ausschließlich allgemeinen Informationszwecken und stellen keine vertraglichen oder sonstigen Verpflichtungen dar. Obwohl die Inhalte sorgfältig geprüft wurden, übernimmt Eye Security keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte. Jegliche Haftung, insbesondere für direkte oder indirekte Schäden, die aus der Nutzung oder Nichtnutzung der Informationen entstehen, ist im gesetzlich zulässigen Umfang ausgeschlossen. Alle Leistungsbeschreibungen unterliegen den geltenden Vertragsbedingungen, Ausschlüssen und Konditionen. Diese Veröffentlichung ersetzt keine individuelle Beratung oder vertragliche Vereinbarungen.

Eye Security: MDR mit Nachrichtendienst-Expertise und eigener Sicherheitsforschung

Eye Cyber Guard verbindet KI-gestützte Angriffserkennung mit einem europäischen 24/7-SOC und Incident Response, ergänzt durch strategische Beratung und Cyberversicherung

Nürnberg, 27. Oktober 2026. Angriffe erkennen, verdächtige Aktivitäten untersuchen und rechtzeitig eingreifen: Mit seinem Managed-Detection-and-Response-Angebot **Eye Cyber Guard** unterstützt Eye Security mehr als 1.000 Unternehmen in Europa. Das Unternehmen verbindet die kontinuierliche Überwachung von Endgeräten, Identitäten und Cloud-Diensten mit der Expertise eines europäischen Security Operations Center (SOC). Eigene Sicherheitsforschung liefert zusätzliche Erkenntnisse über Schwachstellen und Angriffsmethoden.

Gegründet wurde Eye Security 2020 in Den Haag von Job Kuijpers, Vincent van de Ven und Piet Kerkhofs, die zuvor für niederländische Nachrichten- und Sicherheitsdienste tätig waren. Ihre Erfahrung bildet die Grundlage für einen Ansatz, bei dem automatisierte Erkennung und menschliche Untersuchung eng zusammenarbeiten: KI und Sicherheitstechnologien werten Signale aus den überwachten Umgebungen aus. Fachleute prüfen verdächtige Vorgänge, bewerten deren Tragweite und leiten Gegenmaßnahmen ein. Bei einem gemeldeten Sicherheitsvorfall ist laut Eye Security innerhalb von vier Minuten eine erste Ansprechperson aus dem Incident-Response-Team verfügbar.

Eigene Forschung stärkt die operative Abwehr

Mit Eye Research untersucht das Unternehmen Software auf Sicherheitslücken und analysiert neue Angriffsmethoden. Im September 2026 veröffentlichte das Team die Analyse einer kritischen Schwachstellenkette im ASUS Control Center. Ein KI-Agent unterstützte die Untersuchung der Software; die Forschenden prüften die Hinweise, verbanden die einzelnen Schwachstellen zu einer vollständigen Angriffskette und meldeten den Fund an ASUS. Der Hersteller stellte ein Sicherheitsupdate bereit.

Auch bei Microsoft-Technologien hat Eye Security relevante Schwachstellen und Angriffe aufgedeckt. Chief Hacker Vaisha Bernard meldete im vierten Quartal 2025 insgesamt 52 wichtige und kritische Sicherheitslücken und erreichte damit Platz eins auf dem weltweiten Forscher-Ranking des Microsoft Security Response Center. Im selben Jahr identifizierte Eye Research Angriffe auf eine kritische SharePoint-Schwachstelle, als deren Ausnutzung gerade begann. Erkenntnisse aus diesen Untersuchungen fließen in die Weiterentwicklung der Angriffserkennung und Abwehr ein.

„Dieses Ergebnis spiegelt unseren Ansatz wider: Annahmen hinterfragen, Testmethoden konsequent weiterentwickeln und den Fokus klar auf Risiko- und Impact-Minimierung legen“, sagt Bernard über seinen Spitzenplatz im Microsoft-Ranking. Auf der it-sa in Nürnberg gibt der Sicherheitsforscher Einblick in seine Arbeit.

MDR, Incident Response und Beratung aus einem Team

Eye Cyber Guard verbindet die laufende Überwachung mit der Untersuchung und Reaktion auf Sicherheitsvorfälle. Das Team hilft, Angriffe einzugrenzen, den Zugriff der Täter zu unterbinden und betroffene Systeme sicher wieder in Betrieb zu nehmen. Die Zusammenarbeit zwischen SOC

und Incident Response ermöglicht es, Erkenntnisse aus der überwachten Umgebung unmittelbar für die Bearbeitung eines Vorfalls zu nutzen.

Mit Eye vCISO ergänzt Eye Security die operative Abwehr um strategische Beratung. Unternehmen können ihre Sicherheitslage bewerten, Lücken identifizieren und einen priorisierten Maßnahmenplan für die kommenden zwölf Monate entwickeln. Dazu gehört auch die Vorbereitung auf Anforderungen wie NIS2. Eine integrierte Cyberversicherung unterstützt bei den finanziellen Folgen versicherter Vorfälle.

„Europa braucht souveräne Cybersicherheitslösungen, die auf der Erfahrung aus der Nachrichtendienstarbeit, vertrauenswürdiger Technologie, schnellem Handeln und nahtloser Cyberversicherung aufbauen", sagte Gründer und CEO Job Kuijpers anlässlich der Finanzierungsrunde des Unternehmens im Juni 2026. Eye Security verbindet dafür technische Erkennung, fachliche Untersuchung, operative Reaktion und finanzielle Absicherung in einem gemeinsamen Angebot.

Über Eye Security

Eye Security unterstützt kleine und mittelständische Unternehmen dabei, Cyberrisiken ganzheitlich zu erkennen und die operative Resilienz nachhaltig zu stärken. Als führender europäischer MDR-Anbieter kombiniert Eye Security modernste Cybertechnologie mit umfassender Expertise sowie einem nahtlos integrierten Cyberversicherungsschutz. Über 1000 europäische Kunden vertrauen auf die ganzheitliche Schutzlösung, um auch auf unerwartete Cybervorfälle optimal vorbereitet zu sein.

Pressekontakt:
Griffel & Co GmbH
Forsmannstr. 8b, 22303 Hamburg
Janine Griffel
jg@griffel-co.com

Eye Security und HarfangLab bündeln Kräfte: Europäische EDR-Technologie trifft auf ein 24/7-SOC in der EU

Unternehmen können künftig die in Europa entwickelte EDR-Plattform von HarfangLab mit dem 24/7-SOC von Eye Security kombinieren. Die Daten werden in der EU gespeichert. Der Service ist auf Deutsch, Niederländisch und Englisch verfügbar.

Den Haag/Berlin, 27. Oktober 2026 – Unternehmen erhalten künftig eine Cybersicherheitslösung, bei der Technologie, Daten und Einsatzteams in Europa verankert sind. Eye Security und HarfangLab bündeln die Endpoint-Detection-and-Response-Plattform (EDR) von HarfangLab mit dem Managed-Detection-and-Response-Service (MDR) von Eye Security. Dieser umfasst ein rund um die Uhr besetztes europäisches Security Operations Center (SOC) und Incident Response. Eine begrenzte Beta-Phase ist für das vierte Quartal 2026 vorgesehen. Eine breitere Markteinführung ist für Anfang 2027 geplant.

Die Partnerschaft vereint Expertise aus den Bereichen der nationalen Nachrichtendienste und der Cyberabwehr. „Unsere Gründer haben ihre berufliche Laufbahn dem Schutz der nationalen Sicherheit gewidmet. Wir haben Eye Security gegründet, um dieses Fachwissen auch den Unternehmen zugänglich zu machen, auf die Europa angewiesen ist: Krankenhäusern, Industrieunternehmen und Logistikdienstleistern“, sagt Job Kuijpers, CEO und Mitgründer von Eye Security. „Europäische Souveränität bedeutet, frei wählen zu können, ohne Kompromisse beim Schutz eingehen zu müssen. Gemeinsam mit HarfangLab verbinden wir europäisch entwickelte Technologie mit Sicherheitsexperten, die Bedrohungen rund um die Uhr überwachen, untersuchen und darauf reagieren.“

HarfangLab verarbeitet Daten und trainiert seine KI-Modelle unternehmensintern. Die Daten werden innerhalb der EU gespeichert. Die umfassende Workspace Detection and Response-Plattform des Unternehmens schützt moderne IT-Arbeitsumgebungen, von KI-Agenten und digitalen Identitäten über Endgeräte und Cloud-Umgebungen bis hin zu Servern. Die Plattform basiert auf innovativen Technologien zur Erkennung und Abwehr von Cyberbedrohungen, die seit 2018 kontinuierlich weiterentwickelt werden. Die EDR-Lösung erzielte bei unabhängigen Evaluierungen, darunter die MITRE ATT&CK Evaluations und das EDR Telemetry Project, überzeugende Ergebnisse bei der Erkennung von Bedrohungen und der Erkennungsgenauigkeit.

Eye Security entschied sich nach umfangreichen Tests der EDR-Lösung für HarfangLab. Ausschlaggebend waren insbesondere die umfangreichen Telemetriedaten, die leistungsfähigen Möglichkeiten zur aktiven Reaktion auf Bedrohungen sowie die geringe
Beide Partner verfügen über Systembelastung.

Unternehmen können HarfangLab künftig ergänzend zu bereits eingesetzten, kompatiblen EDR-Lösungen nutzen, darunter auch Produkte US-amerikanischer Anbieter. Die Partnerschaft erweitert damit die Wahlmöglichkeiten, ohne dass sie ihre bestehende Sicherheitstechnologie unmittelbar ersetzen müssen.

„Unsere Kunden fragen gezielt nach europäischen Sicherheitslösungen. Sie möchten wissen, woher die eingesetzte Software stammt und wo ihre Daten gespeichert werden“, sagt Ze'ev Rozov, Chief Business Officer bei Eye Security. „Mit HarfangLab bieten wir ihnen eine leistungsfähige europäische EDR-Alternative. Den Übergang können sie an ihren betrieblichen Anforderungen ausrichten.“

Anerkennungen und Zertifizierungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI). Eye Security ist vom BSI offiziell als qualifizierter Dienstleister für die Reaktion auf Advanced Persistent Threats (APT) anerkannt. Der EDR-Agent von HarfangLab wurde nach einer unabhängigen Prüfung im Rahmen des BSZ-Verfahrens des BSI zertifiziert. Darüber hinaus verfügt

die EDR-Lösung von HarfangLab über eine Zertifizierung und Qualifizierung durch die Cybersicherheitsbehörde ANSSI.

Für HarfangLab eröffnet die Partnerschaft neue Möglichkeiten, seine Technologie weiteren Unternehmen in Europa bereitzustellen. „Europas Cyberresilienz hängt davon ab, technische Fähigkeiten in wirksamen Schutz zu überführen", sagt Anouck Teiller, stellvertretende CEO von HarfangLab. „Gemeinsam mit Eye Security verbinden wir in Europa entwickelte Endgerätesicherheit mit Expertinnen und Experten, die rund um die Uhr untersuchen und reagieren. So erhalten mittelständische Unternehmen echte Wahlfreiheit: europäische Technologie, in der EU gehostete Daten und europäische Teams, die für die Reaktion verantwortlich sind."

Als nächsten Schritt plant Eye Security, HarfangLab in sein Agentic SOC zu integrieren. Damit soll die proaktive Suche nach Bedrohungen und Schwachstellen auf Basis europäischer EDR-Technologie erweitert werden. Die Integration wird außerdem die Asset-Discovery-Funktionen von HarfangLab nutzen, um nicht überwachte Assets sichtbar zu machen und Shadow IT sowie Lücken in der Endgeräteüberwachung besser aufzuzeigen.

Die Partnerschaft wird auf der IT-Sicherheitsmesse it-sa in Nürnberg bekannt gegeben. Unternehmen, die an der Betaphase im vierten Quartal 2026 interessiert sind, können sich an Eye Security wenden, um eine mögliche Teilnahme und ihre Anforderungen an die Implementierung zu besprechen.

Über Eye Security
Eye Security bietet Europas am schnellsten wachsende Cybersecurity-Plattform für den Mittelstand. Die Lösung verbindet fortschrittliche KI-Technologie, Managed Detection and Response (MDR) mit einem europäischen 24/7-SOC sowie Incident Response. Eye Security schützt mehr als 1.000 mittelständische Unternehmen in Europa.

Über HarfangLab
HarfangLab ist ein führender europäischer Anbieter im Bereich Workspace Detection and Response. Sicherheitsteams stehen vor der Herausforderung, zahlreiche unterschiedliche Tools zu verwalten. Dadurch können Sicherheitslücken bei KI-Agenten, digitalen Identitäten, Cloud-Umgebungen, öffentlich erreichbaren IT-Ressourcen und Endgeräten entstehen oder verstärkt werden. HarfangLab begegnet dieser Herausforderung mit einer einheitlichen Plattform. Diese basiert auf einem einzigen ressourcenschonenden Agenten und speziell für die Cybersicherheit entwickelter KI. Die von ANSSI und BSI zertifizierte sowie von Gartner und Forrester anerkannte Lösung erweitert die Erkennung und Abwehr von Bedrohungen auf moderne Arbeitsumgebungen – von lokalen IT-Infrastrukturen bis in die Cloud, unabhängig davon, wo gearbeitet wird.

Pressekontakt:
Griffel & Co GmbH
Forsmannstr. 8b, 22303 Hamburg
Janine Griffel
jg@griffel-co.com

HarfangLab
Tyto PR
Amelie Tanzberger & Anniek De Hoop
harfanglab@tytopr.com

Wenn Hacker Sicherheitslücken schließen helfen: Vaisha Bernard spricht auf der it-sa

Der Chief Hacker von Eye Security erreichte Platz eins im weltweiten Microsoft-Ranking für Sicherheitsforschende

Nürnberg, Oktober 2026. Wer eine Sicherheitslücke entdeckt, kann sie ausnutzen – oder dafür sorgen, dass sie geschlossen wird. Vaisha Bernard hat sich auf Letzteres spezialisiert. Der Chief Hacker des europäischen Cybersicherheitsunternehmens Eye Security untersucht Software auf Schwachstellen und meldet seine Funde verantwortungsvoll an die Hersteller. Auf der it-sa in Nürnberg spricht er über seine Arbeit.

Wie ergiebig diese Suche sein kann, zeigte sich im vierten Quartal 2025: Bernard erreichte Platz eins auf dem *Security Researcher Leaderboard* des Microsoft Security Response Center (MSRC). Innerhalb eines Quartals meldete er 52 wichtige und kritische Sicherheitslücken in Microsoft-Technologien. Solche Hinweise geben dem Hersteller die Möglichkeit, Schwachstellen zu prüfen und zu beheben, bevor Angreifer sie ausnutzen. „Dieses Ergebnis spiegelt unseren Ansatz wider: Annahmen hinterfragen, Testmethoden konsequent weiterentwickeln und den Fokus klar auf Risiko- und Impact-Minimierung legen", sagt Bernard.

Sicherheitsforschung als Teil der Abwehr

Microsoft arbeitet über sein Security Response Center mit Forschenden aus aller Welt zusammen. Ihre Meldungen helfen dabei, Risiken in weit verbreiteten Produkten und Diensten zu erkennen. Bernards Spitzenplatz macht sichtbar, welchen Beitrag europäische Sicherheitsforschung zu dieser Zusammenarbeit leisten kann.

Bei Eye Security fließen Erkenntnisse aus der eigenen Sicherheitsforschung in die Weiterentwicklung des Managed-Detection-and-Response-Angebots Eye Cyber Guard ein. Es verbindet die kontinuierliche Überwachung von Endgeräten, Identitäten und Cloud-Diensten mit der Untersuchung und Reaktion durch Fachleute im europäischen Security Operations Center. Die Forschung liefert dabei Wissen darüber, wie Angreifer Schwachstellen ausnutzen und welche Spuren sie hinterlassen. Dieses Verständnis unterstützt die operative Abwehr: verdächtige Aktivitäten frühzeitig erkennen, ihren Zusammenhang untersuchen und Maßnahmen einleiten, um die Folgen eines Angriffs zu begrenzen.

Über Eye Security

Eye Security unterstützt kleine und mittelständische Unternehmen dabei, Cyberrisiken ganzheitlich zu erkennen und die operative Resilienz nachhaltig zu stärken. Als führender europäischer MDR-Anbieter kombiniert Eye Security modernste Cybertechnologie mit umfassender Expertise sowie einem nahtlos integrierten Cyberversicherungsschutz. Über 1000 europäische Kunden vertrauen auf die ganzheitliche Schutzlösung, um auch auf unerwartete Cybervorfälle optimal vorbereitet zu sein.

Pressekontakt:
Griffel & Co GmbH
Forsmannstr. 8b, 22303 Hamburg
Janine Griffel
jg@griffel-co.com

Fabian Lochmann wird Cybersecurity Evangelist bei Eye Security

Erfahrener Security-Operations-Experte übernimmt die fachliche Kommunikation und Partnerunterstützung in der DACH-Region

Berlin, 27. Oktober 2026. Eye Security verstärkt sein Team in der DACH-Region: Fabian Lochmann ist seit Oktober als Cybersecurity Evangelist für das europäische Cybersicherheitsunternehmen tätig. Er wird Eye Security auf Fachveranstaltungen vertreten, über aktuelle Angriffsmethoden und Cybervorfälle sprechen und Partner dabei unterstützen, komplexe Sicherheitsthemen für ihre Kunden einzuordnen.

Lochmann arbeitet seit 2013 in Security Operations. Er hat Systeme zur Auswertung von Sicherheitsereignissen aufgebaut und betrieben, Schadsoftware analysiert, digitale Spuren forensisch untersucht sowie Security Operations Center und Umgebungen für Managed Detection & Response mitentwickelt. Zu seiner Arbeit gehörte auch die Koordination von Sicherheitsvorfällen. Vor seinem Wechsel zu Eye Security war er unter anderem als Manager, Security Services bei Arctic Wolf tätig. Sein fachlicher Schwerpunkt liegt auf der Frage, wie Angreifer in Systeme gelangen, sich darin bewegen und welche Spuren sie hinterlassen. Diese Perspektive bringt Lochmann künftig in Vorträge, Fachgespräche und die Zusammenarbeit mit Partnern von Eye Security ein. Dabei greift er auf Fälle zurück, die er selbst untersucht oder begleitet hat.

„Aus dieser Arbeit stammen die Fälle, die ich auf der Bühne erzähle: reale Angriffe, die ich selbst untersucht oder begleitet habe, keine Beispiele aus zweiter Hand. Was ich vorne sage, habe ich vorher im Log gesehen", sagt Lochmann.

Für Eye Security verbindet die neue Position technische Erfahrung mit öffentlicher Vermittlung. Das Unternehmen überwacht die IT-Umgebungen seiner Kunden rund um die Uhr und kombiniert automatisierte Angriffserkennung mit der Untersuchung und Reaktion durch Sicherheits-expertinnen und -experten. Lochmann soll diese Arbeit in der DACH-Region anhand konkreter Angriffsfälle erläutern und den fachlichen Austausch mit Unternehmen und Partnern ausbauen.

Auch außerhalb seines Berufs beschäftigt sich Lochmann mit der Frage, wie Kommunikation in Krisen funktioniert. Beim Deutschen Roten Kreuz ist er im Sanitätsdienst aktiv und engagiert sich für den Aufbau eines Notfunknetzes im Raum Hildesheim. Die Technik soll den Informations-austausch unterstützen, wenn Mobilfunk oder Internet ausfallen. Lochmann ist zudem stellvertretender Kreisbereitschaftsleiter beim DRK.

Über Eye Security

Eye Security unterstützt kleine und mittelständische Unternehmen dabei, Cyberrisiken ganzheitlich zu erkennen und die operative Resilienz nachhaltig zu stärken. Als führender europäischer MDR-Anbieter kombiniert Eye Security modernste Cybertechnologie mit umfassender Expertise sowie einem nahtlos integrierten Cyberversicherungsschutz. Über 1000 europäische Kunden vertrauen auf die ganzheitliche Schutzlösung, um auf unerwartete Cybervorfälle optimal vorbereitet zu sein.

Pressekontakt:
Griffel & Co GmbH
Forsmannstr. 8b, 22303 Hamburg
Janine Griffel
jg@griffel-co.com

Eye on Cybersecurity

Forschung, die weiterdenkt. Sicherheit, die Schritt hält.



Cybersecurity im Fokus: KI verändert Angriff und Abwehr

Liebe Leserinnen und Leser,

KI hilft Kriminellen, gestohlene Postfächer auszuwerten. Sie unterstützt Sicherheitsforscher bei der Suche nach komplexen Schwachstellen. Und ihre Nutzung im Arbeitsalltag stellt Unternehmen vor neue Datenrisiken.

In dieser Ausgabe zeigen wir, wie Phishing-Plattformen E-Mail-Betrug automatisieren, warum nach der WordPress-Schwachstelle wp2shell ein Update allein nicht reicht und wie Unternehmen vertrauliche Informationen bei der KI-Nutzung schützen können. Wir verbinden Erkenntnisse aus unserer Forschung mit konkreten Ansätzen für die Abwehr.

Piet Kerkhofs
CTO & Mitgründer, Eye Security

KI-gestützte Phishing-Plattformen erleichtern den Betrug mit Geschäftsmails

Angreifer müssen nicht mehr jeden Schritt selbst beherrschen. Neue Plattformen bündeln Kontozugriff, Postfachanalyse und Betrugsvorbereitung in einer Oberfläche. Für Unternehmen verändert sich damit die Bedrohung hinter einer scheinbar gewöhnlichen E-Mail.

Die Rechnung kommt von einem bekannten Geschäftspartner. Der Ton stimmt, das Projekt ist vertraut, die Zahlungsaufforderung passt zum bisherigen Austausch. Nur die Bankverbindung ist neu. Wer hier nach Rechtschreibfehlern oder einem verdächtigen Absender sucht, kann lange suchen: Die Nachricht stammt möglicherweise aus einem tatsächlich übernommenen Postfach.

Business Email Compromise, kurz BEC, nutzt genau dieses Vertrauen. Angreifer verschaffen sich Zugang zu geschäftlichen E-Mail-Konten, um Kommunikation auszuspähen und beispielsweise Zahlungen umzuleiten. KI hilft ihnen inzwischen dabei, die Informationen hinter dem Zugang schneller auszuwerten.

Phishing-Plattformen verwalten gestohlene Konten

Das Forschungsteam von Eye Security hat zwei Phishing-Kits untersucht, deren Oberflächen an reguläre Softwaredienste erinnern: mit unterschiedlichen Nutzerrollen, Verwaltungsfunktionen und automatisierten Abläufen. Nach Einschätzung der

Forschenden weist der Code deutliche Spuren KI-gestützter Entwicklung auf.

Eines der Kits enthält außerdem eine KI-Komponente, die erbeutete Postfächer auf Rechnungen, offene Forderungen und Zahlungsprozesse untersucht. Damit wird ein arbeitsintensiver Teil des Betrugs automatisiert: herauszufinden, wo Geld fließt und an welcher Stelle sich eine Kommunikation manipulieren lässt.

Die einzelnen Angriffstechniken sind überwiegend bekannt. Neu ist ihre Bündelung. Eine gemeinsame Oberfläche erleichtert es auch weniger erfahrenen Anwendern, mehrere kompromittierte Konten zu verwalten und nach finanziell interessanten Vorgängen zu durchsuchen.

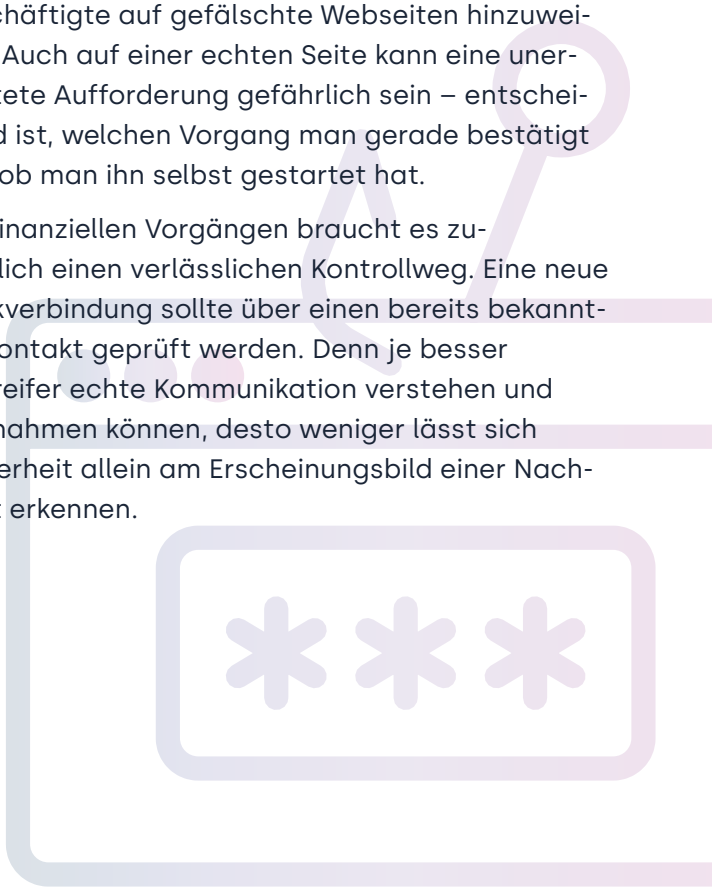
Device Code Phishing missbraucht die Microsoft-Anmeldung

Zum Einsatz kommt dabei unter anderem Device Code Phishing. Dieses Verfahren missbraucht einen legitimen Anmeldeweg, der beispielsweise für Geräte ohne komfortable Eingabemöglichkeit ‘vorgesehen ist. Nutzer geben einen kurzen Code auf einer offiziellen Microsoft-Seite ein und bestätigen die Anmeldung. Beim Angriff stammt dieser Code jedoch aus einem Vorgang, den der Täter gestartet hat. Das Opfer autorisiert damit dessen Sitzung.

Dass diese Methode im großen Maßstab eingesetzt wird, zeigt Microsofts Untersuchung der Plattform EvilTokens. Das Unternehmen empfiehlt, den zugrunde liegenden Anmeldeweg nach Möglichkeit zu sperren und notwendige Ausnahmen gezielt einzugrenzen.

Für Unternehmen reicht es deshalb nicht, Beschäftigte auf gefälschte Webseiten hinzuweisen. Auch auf einer echten Seite kann eine unerwartete Aufforderung gefährlich sein – entscheidend ist, welchen Vorgang man gerade bestätigt und ob man ihn selbst gestartet hat.

Bei finanziellen Vorgängen braucht es zusätzlich einen verlässlichen Kontrollweg. Eine neue Bankverbindung sollte über einen bereits bekannten Kontakt geprüft werden. Denn je besser Angreifer echte Kommunikation verstehen und nachahmen können, desto weniger lässt sich Sicherheit allein am Erscheinungsbild einer Nachricht erkennen.



WordPress-Schwachstelle wp2shell: Warum ein Update allein nicht reicht

Die WordPress-Angriffskette wp2shell zeigt, wie KI Sicherheitsforschung verändert. Für betroffene Unternehmen bleibt anschließend eine Frage offen, die kein Update allein beantworten kann: Wurde die Schwachstelle bereits ausgenutzt?

Eine Website funktioniert, das Sicherheitsupdate ist installiert, der Betrieb läuft weiter. Aus Sicht des Unternehmens scheint der Vorfall damit erledigt. Doch ein geschlossener Zugang sagt wenig darüber aus, was zuvor passiert ist.

Diese Unterscheidung stand im Mittelpunkt der Arbeit von Eye Security an wp2shell. Die im Juli veröffentlichte Angriffskette betraf den WordPress-Kern. Unter den beschriebenen Voraussetzungen konnten Angreifer ohne Anmeldung Administratorrechte erlangen und Code ausführen. Zusätzliche Plug-ins oder besondere Themes waren dafür nicht erforderlich.

Wie KI die Angriffskette aufdeckte

Entdeckt wurde die Kette von Adam Kues bei Searchlight Cyber mithilfe eines KI-Modells. In seinem Bericht beschreibt er einen mehrstufigen Prozess: Er ließ den Quellcode untersuchen, prüfte einen zunächst überraschenden Fund an einer

Testinstallation und ließ anschließend analysieren, ob sich der Zugriff weiter ausbauen ließ.

Die KI lieferte dabei technische Ergebnisse, deren Tragweite der Forscher erst nachvollziehen und überprüfen musste. Nach der Entdeckung folgten die Aufarbeitung der Angriffskette und die Meldung an WordPress. Der Fall zeigt, dass KI inzwischen auch bei anspruchsvollen Untersuchungen einen konkreten Beitrag leisten kann – und wie viel menschliche Arbeit trotzdem zwischen einem gemeldeten Fund und einer belastbaren Sicherheitsanalyse liegt.

Nach dem Update auf Angriffsspuren prüfen

Eye Security entwickelte für die anschließende Abwehr einen Untersuchungsleitfaden und zwei kostenlose Werkzeuge. Eine Browser-Erweiterung unterstützt die erste Einschätzung, ob eine Website einen abgesicherten Versionsstand erkennen lässt. Ein WordPress-Plug-in sucht nach bekannten Spuren der Angriffskette.

Diese Spuren sind wichtig, weil ein Update einen zuvor erfolgten Einbruch nicht rückgängig macht. Ebenso wenig beweist ein unauffälliger Scan, dass es keinen Angriff gab: Prüfwerkzeuge erkennen bestimmte Merkmale, und sorgfältig beseitigte Spuren können ihrer Suche entgehen.

Die praktische Lehre reicht über WordPress hinaus. Bei einer kritischen Schwachstelle müssen Unternehmen zwei Aufgaben bewältigen: den verwundbaren Zustand beenden und mögliche Folgen untersuchen. Wer nach dem Update sofort zur Tagesordnung übergeht, beantwortet nur die erste Frage.

Für Sicherheitsverantwortliche bedeutet das, technische Wartung und Vorfallanalyse zusammenzudenken. Ein Update schützt den weiteren Betrieb. Eine Untersuchung klärt, ob bereits etwas zurückgeblieben ist.

Shadow AI: Wenn vertrauliche Unternehmensdaten im privaten KI-Chat landen

Ungeprüfte KI-Nutzung entsteht häufig aus einem ganz normalen Arbeitsauftrag. Wie Unternehmen damit umgehen, entscheidet sich deshalb auch daran, ob sichere Alternativen im Alltag funktionieren.

Der Vertrag ist lang, der nächste Termin beginnt in zehn Minuten. Eine kurze Zusammenfassung wäre hilfreich. Also wird das Dokument in einen KI-Chat kopiert. Wenige Sekunden später liegt das Ergebnis vor. Diese beispielhafte Situation braucht weder einen Angreifer noch böse Absicht. Sie entsteht aus Zeitdruck und dem Wunsch, eine Aufgabe schneller zu erledigen. Trotzdem stellt sie eine Sicherheitsfrage: Darf dieses Dokument an diesen Dienst übermittelt werden?

Private KI-Konten als Datenrisiko

Von Shadow AI spricht man, wenn Beschäftigte KI-Angebote außerhalb der vorgesehenen Unternehmensprozesse nutzen. Das können persönliche Konten bei bekannten Anbietern sein oder neue Dienste, die noch niemand geprüft hat. Vertrauliche Inhalte verlassen dabei möglicherweise die kontrollierte Arbeitsumgebung.

Welche Folgen eine Eingabe hat, lässt sich nicht pauschal beantworten. Speicherung, Zugriffsmöglichkeiten und eine mögliche Nutzung zur Verbesserung von KI-Systemen hängen unter anderem vom Anbieter, Kontotyp und den Einstellungen ab. Gerade deshalb ist die Entscheidung für ein bestimmtes Konto keine reine Komfortfrage. Eye Security hat mit AI Leak Block eine kostenlose Open-Source-Erweiterung entwickelt, die an diesem Moment ansetzt. Sie erkennt auf unterstützten Plattformen bestimmte Kontotypen und unterbricht Anfragen aus persönlichen Konten zunächst. Ein Hinweis kann Beschäftigte zum vorgesehenen Unternehmensangebot führen. Die Verarbeitung erfolgt lokal; Nutzereingaben werden nicht an Eye Security übermittelt. Der Hinweis lässt sich aller-

dings übergehen. Die Erweiterung ist damit eine Hilfestellung und keine lückenlose Kontrolle des Datenabflusses.

Freigegebene KI-Angebote im Alltag nutzbar machen

Aus Unternehmenssicht liegt die Herausforderung deshalb auch in der Organisation. Beschäftigte brauchen verständliche Antworten: Welches Werkzeug darf ich nutzen? Mit welchem Konto? Welche Informationen gehören dort hinein? Und an wen kann ich mich wenden, wenn ich unsicher bin?

Ein freigegebenes Angebot hilft nur, wenn es erreichbar ist und die benötigte Aufgabe unterstützt. Bleibt der sichere Weg umständlich oder unklar, entsteht im Arbeitsalltag schnell ein eigener.

Shadow AI lässt sich deshalb nicht allein mit einem weiteren Hinweis im Intranet bearbeiten. Technische Unterstützung, klare Regeln und brauchbare Angebote müssen zusammenpassen. Die entscheidende Situation ist oft unspektakulär: ein langer Vertrag, wenig Zeit und ein geöffnetes Chatfenster.

Fünf Fragen an Vaisha Bernard:

Wie ein ethischer Hacker Sicherheitslücken aufspürt



Vaisha Bernard sucht nach Sicherheitslücken, bevor andere sie ausnutzen können. Im vierten Quartal 2025 belegte er Platz eins auf dem Security Researcher Leaderboard des Microsoft Security Response Center. Im Interview erklärt er, wie er arbeitet, was KI daran verändert und welchen Blick Unternehmen von einem Hacker übernehmen können.

Dein Jobtitel lautet „Chief Hacker". Wie erklärst du jemandem außerhalb der IT, was du den ganzen Tag machst – und was dich daran begeistert?

„Ich sage immer: Ich werde dafür bezahlt, Dinge kaputt zu machen, bevor es jemand mit schlechteren Absichten tut. Im Kern mache ich seit meinem achten Lebensjahr dasselbe: Ich schaue mir an, wie ein System oder eine Regel gedacht ist – und was passiert, wenn man es anders benutzt, als der Erfinder es vorgesehen hat. Bei meiner Mutter war das ein Strafzettel unter dem Scheibenwischer, den sie sich von einem anderen Auto ‚ausgeliehen' hat, damit sie selbst keinen bekommt. Heute sind es Microsoft-Produkte oder Authentifizierungs-Flows. Das Prinzip ist gleich geblieben, nur die Systeme sind komplexer geworden."

Nimm uns mit in den Moment, in dem du eine neue Sicherheitslücke entdeckst: Was macht dich zuerst misstrauisch, und wie findest du heraus, ob daraus ein ernstes Problem werden kann?

„Der erste Auslöser ist fast nie ein lauter Alarm, sondern etwas Kleines, das nicht zusammenpasst. Ich habe einmal Einstellungen für unsere Phishing-Simulationen automatisiert und gemerkt: Mache ich das zu schnell hintereinander, stimmen die Werte hinterher nicht mehr. Beim genaueren Hinsehen stellte sich heraus, dass ich in einer Race Condition gelandet war und tatsächlich Einstellungen bei fremden Microsoft-Tenants verändert hatte – Organisationen, die nicht einmal unsere Kunden waren. Um den Ernst der Lage einzuschätzen, spiele ich dann konsequent bis zum Ende durch, was das bedeutet: In diesem Fall hatte ich eine vollständige Remote-PowerShell-Sitzung als Compliance Administrator bei einem fremden Tenant – und hätte darüber per eDiscovery sämtliche Dokumente aus SharePoint herunterladen können."

KI kann inzwischen bei der Suche nach komplexen Schwachstellen helfen. Welche Aufgabe hat sie dir zuletzt abgenommen – und bei welcher Frage vertraust du weiterhin auf deine eigene Untersuchung?

„Ich habe tatsächlich mal Astrophysik studiert und bin dann zur KI gewechselt, lange bevor das Mainstream war. Bei der Schwachstellensuche nutze ich KI-Modelle heute, um große Mengen an Code oder Konfigurationen schneller zu sichten. Was sie mir nicht abnimmt: die eigentliche Bewertung, ob ein Fund wirklich ausnutzbar ist und wie weit sich ein Zugriff ausbauen lässt. Das bleibt Handarbeit."

Dein erster Platz auf Microsofts Security Researcher Leaderboard würdigt die Wirkung deiner Forschung. Welcher Fund hat deinen Blick auf Cybersicherheit besonders verändert, und warum?

„Das war der Moment mit den aka.ms-Links – diesen kurzen Microsoft-Verweisen, die man täglich anklickt, ohne nachzudenken. Aus Neugier habe ich aka.ms einmal ganz ohne alles danach aufgerufen und landete auf einem Login-Prompt. Richtig verändert hat meinen Blick, was ich beim Weitergraben fand: eine interne Struktur, über die sich nachvollziehen ließ, welche internen Systeme bei Microsoft überhaupt existieren. Ein unscheinbarer URL-Shortener legte also etwas offen, ein Detail, das auch in großen Organisationen leicht übersehen wird."

Wenn du einen Tag lang die IT eines mittelständischen Unternehmens aus Sicht eines Angreifers betrachten dürftest: Wo würdest du zuerst hinsehen – und was sollten Verantwortliche daraus lernen?

„Ich würde nicht bei der Firewall anfangen, sondern bei den Dingen, die niemand mehr anschaut, weil sie einmal eingerichtet wurden und seither laufen: alte Freigaben, vergessene Testkonten, Ausnahmeregeln in der E-Mail-Sicherheit. Genau dort finde ich in meiner eigenen Arbeit die interessantesten Dinge. Für Verantwortliche heißt das: Sicherheit ist kein Zustand, den man einmal herstellt, sondern etwas, das man regelmäßig neu hinterfragen muss."

Über Eye Security

Eye Security unterstützt kleine und mittelständische Unternehmen dabei, Cyberrisiken ganzheitlich zu erkennen und die operative Resilienz nachhaltig zu stärken. Als führender europäischer MDR-Anbieter kombiniert Eye Security modernste Cybertechnologie mit umfassender Expertise sowie einem nahtlos integrierten Cyberversicherungsschutz. Über 1.000 europäische Kunden vertrauen auf die ganzheitliche Schutzlösung, um auch auf unerwartete Cybervorfälle optimal vorbereitet zu sein. **eyesecurity.de**

Pressekontakt

Janine Griffel, Griffel & Co. GmbH
Forsmannstr. 8b, 22303 Hamburg
jg@griffel-co.com

Incident-Response-Hotline

Rund um die Uhr erreichbar unter **+49 (0)203 6688 1900**
Für nicht dringende Fälle erreichen Sie das IR-Team per E-Mail unter **cert@eye.security**.

© 2026 Eye Security. Alle Rechte vorbehalten. Die in dieser Veröffentlichung enthaltenen Informationen dienen ausschließlich allgemeinen Informationszwecken und stellen keine vertraglichen oder sonstigen Verpflichtungen dar. Obwohl die Inhalte sorgfältig geprüft wurden, übernimmt Eye Security keine Gewähr für die Richtigkeit, Vollständigkeit oder Aktualität der Inhalte. Jegliche Haftung, insbesondere für direkte oder indirekte Schäden, die aus der Nutzung oder Nichtnutzung der Informationen entstehen, ist im gesetzlich zulässigen Umfang ausgeschlossen. Alle Leistungsbeschreibungen unterliegen den geltenden Vertragsbedingungen, Ausschlüssen und Konditionen. Diese Veröffentlichung ersetzt keine individuelle Beratung oder vertragliche Vereinbarungen.