PRESSEINFORMATION

München, 9. Juni 2026

NATO-Cyberabwehrübung Locked Shields 2026

Orange Cyberdefense im zweitplatzierten DACHL-Team von Locked Shields 2026

Zwei IT-Sicherheitsfachleute von Orange Cyberdefense Germany schützten Systeme und wehrten Echtzeitangriffe im Team aus Deutschland, Österreich, der Schweiz und Luxemburg erfolgreich ab

Platz zwei unter 16 multinationalen Teams, dazu jeweils Rang eins in Technischer Cyberabwehr und Strategischer Kommunikation: Das DACHL-Team aus Bundeswehr, österreichischem Bundesheer, Schweizer Armee und luxemburgischen Streitkräften hat bei der NATO-Cyberabwehrübung „Locked Shields 2026“ ein starkes Ergebnis erzielt. Kerstin Hörmann und Jörn Tillmanns von Orange Cyberdefense Germany gehörten zu den über 190 Fachleuten aus Streitkräften, Behörden und Wirtschaft im unter deutscher Führung stehenden Blue Team, das die simulierte Infrastruktur eines fiktiven Staates gegen Echtzeitangriffe verteidigte. Die vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn organisierte Übung, auf der mehr als 4.000 Fachleute aus 41 Nationen teilnahmen, gilt als weltweit größte und komplexeste Live-Fire-Cyberübung.

Vom 20. bis 24. April verteidigten die Blue Teams im Übungshauptquartier in Kalkar simulierte IT-Systeme kritischer Infrastrukturen gegen koordinierte Echtzeitangriffe spezialisierter Red Teams. Die Angriffsszenarien zielten auf Systeme aus verschiedenen Industriesektoren und umfassten realistische Multi-Vektor-Offensiven. Die Angreifer hatten sich über ein Jahr auf die Übung vorbereitet und nutzten neben bekannten Schwachstellen auch eigens entwickelte Werkzeuge und Angriffsmuster, die nicht zuverlässig über bekannte Signaturen oder Indicators of Compromise erkennbar waren. Die IT-Security-Experten von Orange Cyberdefense Germany – Kerstin Hörmann, Managed-SIEM-Expertin, und Jörn Tillmanns, CyberSOC Tech Lead und Senior Security Analyst – arbeiteten in den Sub-Teams für Windows und Web-Applikationen. Ihre Aufgaben waren das Anbinden von Logquellen, die Härtung der zu verteidigenden Systeme sowie die Erkennung und Abwehr laufender Angriffe. „Innerhalb kürzester Zeit mussten Logquellen angebunden und Security-Tools ausgerollt

werden, damit Analysten die Angriffe frühzeitig erkennen und wirksam darauf reagieren können. Hier zählt jede Sekunde“, so Kerstin Hörmann.

Alle drei Kerntechnologien der SOC-Triade kamen während der Übung aktiv zum Einsatz: SIEM (Security Information and Event Management) korrelierte sicherheitsrelevante Logdaten aus der gesamten Infrastruktur, EDR (Endpoint Detection and Response) überwachte die Endgeräte und NDR (Network Detection and Response) analysierte den Netzwerkverkehr in Echtzeit. Da die Angreifer teilweise eigene Tools einsetzten, für die keine Signaturen oder Hashwerte vorlagen, reichte die klassische Erkennung über Indicators of Compromise nicht aus. Das Team musste auf verhaltensbasierte taktische Erkennung setzen, also Angriffsmuster anhand von Taktiken, Techniken und Prozeduren (TTPs) identifizieren. Bewertet wurden die Teams nicht nur für die erfolgreiche Abwehr, sondern auch für die Schadensbehebung nach erfolgreichen Einbrüchen und für das Sammeln und Melden von Cyber Threat Intelligence. „Seit sechs Jahren arbeite ich im Bereich Detection und Response, aber Locked Shields ist eine andere Liga. Die Angriffe sind hochdynamisch, präzise orchestriert und erzeugen permanenten Entscheidungsdruck“, so Jörn Tillmanns.

Für Orange Cyberdefense war es die zweite Teilnahme in Folge. 2025 hatten erstmals drei Mitarbeitende das Unternehmen bei Locked Shields vertreten und gehörten zum Siegerteam von Deutschland und Singapur. 2026 bewies das Unternehmen in neuer Konstellation, dass seine Expertise auch unter veränderten Bedingungen trägt. Den Gesamtsieg sicherte sich knapp ein Team aus Singapur und Lettland. Die Erfahrungen aus der Übung fließen bei Orange Cyberdefense direkt in die operative Arbeit ein, unter anderem in die Konfiguration von SIEM-Systemen, in Detection-Engineering-Prozesse und in die Incident Response für Kunden. Ebenso wertvoll ist der persönliche Kontakt zu Fachleuten aus Streitkräften, Behörden und internationalen Partnerorganisationen, der im Ernstfall schnelle Kommunikation und einen gezielten Austausch von Bedrohungsinformationen ermöglicht. Kerstin Hörmann: „Die Übung spiegelt Angriffsmuster wider, denen Unternehmen in hochregulierten Branchen und im Bereich kritischer Infrastruktur täglich begegnen. Der Unterschied: Bei Locked Shields lassen sich Fehler machen, aus denen wir lernen können, bevor der Ernstfall eintritt.“

Locked Shields 2026

Locked Shields ist die weltweit größte und komplexeste multinationale Cyberabwehrübung. Sie wird seit 2010 jährlich vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estland,

organisiert. Während dieser „Live-Fire Cyber Defence Exercise“ verteidigen internationale Teams in Echtzeit simulierte Computernetzwerke und IT-Systeme kritischer Infrastrukturen (KRITIS) gegen hochentwickelte Cyberangriffe. Die Übung folgt dem Blue-Team-vs.-Red-Team-Prinzip: Das Red Team führt koordinierte, realistische Angriffe durch, während die multinationalen Blue Teams die Verteidigung übernehmen. Neben technischen Fähigkeiten testet die Übung auch rechtliche Bewertungen, strategische Kommunikation und Entscheidungsfindung unter Zeitdruck. Das DACHL-Team übte vom deutschen Standort Kalkar aus und umfasste mehr als 190 Fachleute, davon rund 35 aus Behörden und Wirtschaft.

Abbildung

OCD_KHoermann-JTillmans_CD26.jpg

Kerstin Hörmann und Jörn Tillmanns von Orange Cyberdefense Germany unterstützten das DACHL-Team bei der NATO-Cyberübung Locked Shields 2026 in Kalkar.
(Foto: Orange Cyberdefense Germany)

Das Bildmaterial finden Sie in unserem Medienportal press-n-relations.amid-pr.com zum Download (Suchbegriff „Locked Shields 2026“). Die Dateien erhalten Sie auf Wunsch auch gerne per E-Mail. Kontakt: ut@press-n-relations.de

Weitere Informationen:
Orange Cyberdefense Germany GmbH
Kathrin Helmrich
Team Lead Marketing
Paul-Gerhardt-Allee 24
81245 München
Telefon: +49 170 2144593
kathrin.helmrich@orangecyberdefense.com
www.orangecyberdefense.com

Presse- und Öffentlichkeitsarbeit:
Press’n’Relations GmbH
Uwe Taeger / Rebecca Horn
Magirus-Deutz-Straße 14
89077 Ulm
Telefon: +49 731 146156-71 / -75
ut@press-n-relations.de
rh@press-n-relations.de
https://press-n-relations.de/

Orange Cyberdefense Germany GmbH
Die Orange Cyberdefense Germany GmbH mit Sitz in München ist Teil der globalen Cybersecurity-Einheit der Orange Group. Das Unternehmen bietet umfassende IT-Sicherheitslösungen an, darunter Managed Security Services, Threat Intelligence, Penetration Testing und Incident Response. Mit über 30 Jahren Erfahrung und einem Netzwerk von 3.300 multidisziplinären Experten in zwölf Ländern und 36 Security Operation Centern weltweit schützt Orange Cyberdefense Unternehmen rund um den Globus vor digitalen Bedrohungen. 2025 erzielte das Unternehmen einen Umsatz von 1,3 Milliarden Euro. In Deutschland beschäftigt die GmbH rund 85 Mitarbeitende.