

Datum: 15.10.2026

Betrachtungszeitraum: 24.09. bis 14.10.2026

post@bundesamt-cybersicherheit.gv.at

Lage CYBERSICHERHEIT

NIS2-CRA / Schwachstellen / Angriffsfläche

NIS2/CRA: Mit 01.10.2026 ist das [NISG2026](#) – die **Umsetzung der NIS2-Richtlinie in AT** - in vollem Umfang in Kraft getreten. Details zur Umsetzung, insbesondere zur Registrierung als wichtige oder wesentliche Einrichtung, finden sich auf der [Webseite des neu gegründeten Bundesamtes für Cybersicherheit](#). Mit 11.09.2026 ist die **Meldepflicht von aktiv ausgenutzten Schwachstellen und relevanten Vorfällen** bei Herstellern von Produkten mit digitalen Elementen laut [Cyber Resilience Act](#) wirksam geworden.

Schwachstellen: Auch in den letzten vier Wochen wurde wieder eine **hohe Zahl an Schwachstellen** gemeldet, und es sind wieder Edge-Devices betroffen. Die Serie an [Problemen mit Citrix Netscaler ADC und Netscaler Gateway](#) hat [sich fortgesetzt](#), es kam zur aktiven **Ausnutzung von mehreren 0-day Schwachstellen**. Betroffen waren auch Systeme von [Fortinet](#), [Check Point](#) und [Ivanti](#). Aktuell gilt, dass es kein sicheres Zeitfenster mehr für Patches gibt, die Ausnutzung der Schwachstellen startet immer öfter vor der Verfügbarkeit der Patches. Umso wichtiger ist es, dass **neben schnellem Patchen auch die Voraussetzungen für eine umfassende Reaktion** gegeben sind: Dazu gehört, dass Logs zentral gesammelt werden (im Fall der Citrix 0-days wurden die Spuren am Gerät gelöscht) und dass eine WAF zur Protokollierung auf http-Ebene eingesetzt wird.

Angriffsfläche: Je weniger Systeme direkt aus dem Internet erreichbar sind, umso weniger ist eine Massenausnutzung möglich. Das gilt neben den hier schon oft erwähnten **Managementinterfaces** (etwa Check Point Management Server oder VMware vCenter) auch für jede Form von [Industrial Control Systems \(ICS\)](#). So wurden in der Nacht von 11./12.10.2026 in FR die [Kühlanlagen diverser Einzelhandelsketten](#) so manipuliert, dass Gefriergut aufgeheizt und damit unbrauchbar gemacht wurde. Schuld waren hier [ungesicherte Fernwartungszugänge von Geräten mehrerer Hersteller](#). Achtung, manche dieser Systeme kommunizieren anstatt über die eigene, gemanagte Netzwerkinfrastruktur direkt über Mobilfunk.

Lage CYBERCRIME

Cyberkriminalität

Ransomware: Es wurden **Angriffe durch Verschlüsselungstrojaner** registriert, bei denen zur Erhöhung des Drucks auf die Opfer auch die **Backups gelöscht** wurden. In diesen Fällen wurden **Lösegeldforderungen in Höhe von bis zu 100.000 Euro** gestellt.

Internetbasierte(r) Erpressung/Betrug: Es wurde eine **Zunahme von „MS Support Scams“** unter Verwendung von AnyDesk sowie diverse Fälle von Bestellbetrug verzeichnet. Des Weiteren kam es zu **Erpressungen mittels der Androhung der Veröffentlichung von Intimbildern** sowie zu **betrügerischen Aktivitäten** durch KI-generierte Videos (Deepfakes) zur unbefugten Geldbeschaffung. Zudem wurden **Manipulationen von E-Mails** zur Änderung von IBAN-Daten, ein **signifikant hohes Aufkommen an WhatsApp-Phishing** sowie Fälle von „**Ghost Pairing**“ registriert.

Widerrechtliche Zugriffe auf Accounts: Es wurden **unbefugte Zugriffe auf Accounts** verschiedener Plattformen gemeldet. Ein **besonders hohes Aufkommen an Angriffen wurde bei WhatsApp** festgestellt. In den meisten Fällen beschränkte sich die Täterschaft auf die Sperrung der Accounts, ohne dass weitere Tathandlungen vorgenommen wurden.

Datum: 15.10.2026

Betrachtungszeitraum: 24.09. bis 14.10.2026

post@bundesamt-cybersicherheit.gv.at

Verletzung der Persönlichkeitssphäre: Die Meldungen betrafen **diverse Formen der Bloßstellung, Diffamierung und Beschimpfung** im Internet. Hierzu zählte die Verbreitung von **Aufnahmen geschlechtlicher Handlungen** sowie die **Distribution von Intimaufnahmen** im schulischen Umfeld. Zudem wurden Fälle registriert, in denen **KI-generierte intime Szenen** zur Diffamierung von Schülern in größeren Gruppen verwendet wurden, sowie die **Erstellung von Fake-Webseiten** mit herabwürdigenden Inhalten.

Technologiebasierte Angriffe: Die registrierten Vorfälle umfassten **Datendiebstähle von Servern** im Gastronomiebereich, sowie **unbefugte Zugriffe** auf Server einer Universität. Des Weiteren wurden **Angriffe auf Druckersysteme** mittels „Remote Code Execution“ (Fernausführung von Programmcode) sowie **DDoS-Attacken** (Distributed Denial of Service) verzeichnet.

Lage INTERNATIONAL

JP / International / US

JP: Am 01.10.2026 trat die [neue Gesetzgebung zu aktiver Cyberverteidigung](#) in Kraft. Damit haben Polizei und Militär die Befugnis, **präemptiv gegen Cyberangriffe vorzugehen**: Wenn Anzeichen für einen bevorstehenden Angriff bestehen, können die Sicherheitskräfte aktiv in andere Server eindringen, um die Bedrohung zu neutralisieren, z.B. indem sie Programme löschen. Die Aufsicht liegt bei der „Active Cyber Defense Oversight Commission“, die als unabhängige Kommission die Verhältnismäßigkeit der gesetzten Maßnahmen beurteilen soll.

International: Microsoft berichtet, dass die seit Mai 2026 beobachtete Kampagne [„CaptiveCrunch“](#) von Storm-2945, einem Teil von Midnight Blizzard (SVR), Reisende über manipulierte Captive Portals in Hotel- und Gastnetzwerken angreift. Gefälschte Updates und ClickFix-Anweisungen verbreiten Malware, die **Zugangsdaten, Sitzungscookies und Tokens stiehlt**. Laut Update vom 05.10.2026 wurde die Kampagne am 29.09.2026 wieder aufgenommen. Es sollten **Gast- bzw. Hotel-WLANs als nicht vertrauenswürdig behandelt**, Downloads daraus blockiert und Phishing-resistente MFA-Authentifizierung sowie strenge Anmelderichtlinien umgesetzt werden.

US: Am 29.09.2026 richtete Präsident Trump eine [„Super Intelligence Force“](#) ein, die auch ein umfassendes **Mandat im Bereich der Cybersicherheit** hat. Die Task Force unter Leitung des neuen KI-Beraters Jay Clayton soll innerhalb von 120 Tagen **Chancen und Risiken fortgeschrittener KI untersuchen**, darunter Cybersicherheit, Schutz bürgerlicher Freiheiten und mögliche Sicherheitsanforderungen an KI-Anbieter. Die Regierung hält an einem innovationsfreundlichen, regulatorisch zurückhaltenden Ansatz fest, verstärkt angesichts neuer Vorfälle mit autonomen KI-Agenten jedoch die Diskussion über Sicherheitsüberprüfungen und freiwillige Branchenstandards. Bereits am 29.09.2026 hatte Trump per Dekret die Verwendung der **Bezeichnung „Super Intelligence“ statt „Artificial Intelligence“** innerhalb der Exekutive [angeordnet](#).

LAGEBILD FEEDBACK | Wir schätzen Ihre Meinung: [Bitte hier klicken!](#)