WEBINAR: PATCHING IM KI-ZEITALTER –
MIT PRAXIS-BEISPIEL BEI DER KRANKENKASSE SLKK: AUTOMATISIERTE UPDATES VON ENDPOINTS UND SERVERN

first frame networkers



HERZLICH WILLKOMMEN

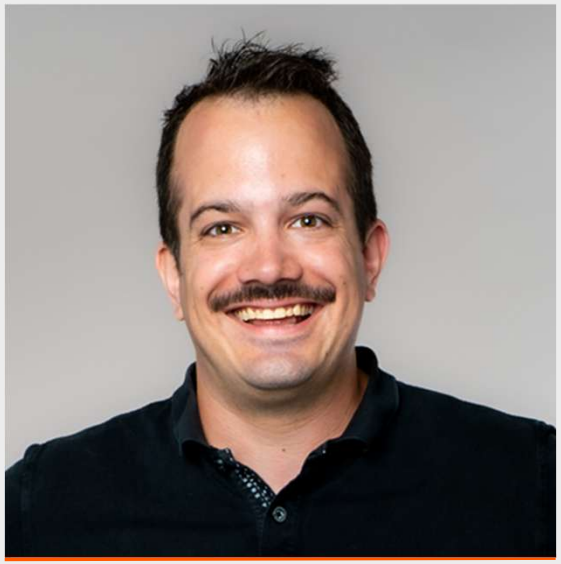
first frame networkers

Vielen Dank, dass Sie sich die Zeit für uns nehmen!

Was Sie heute erwartet:

Praxis-Beispiel bei der Krankenkasse SLKK:
Automatisierte Updates von Endpoints und Servern.

Das Webinar wird in Schweizerdeutsch gehalten.

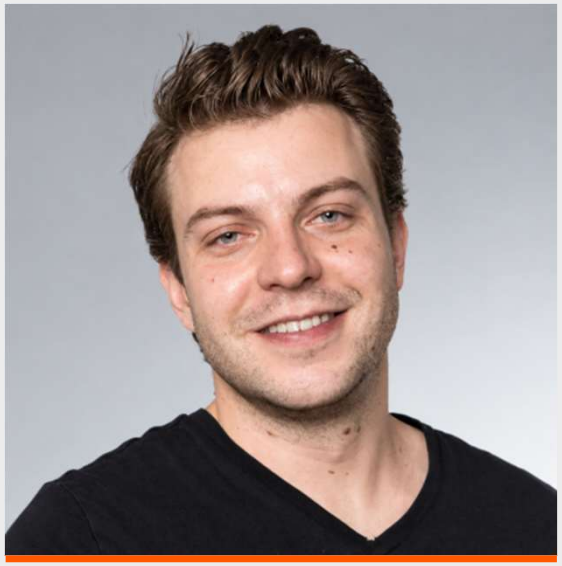


PHILIPPE HIRZEL

Projektleiter Security Services

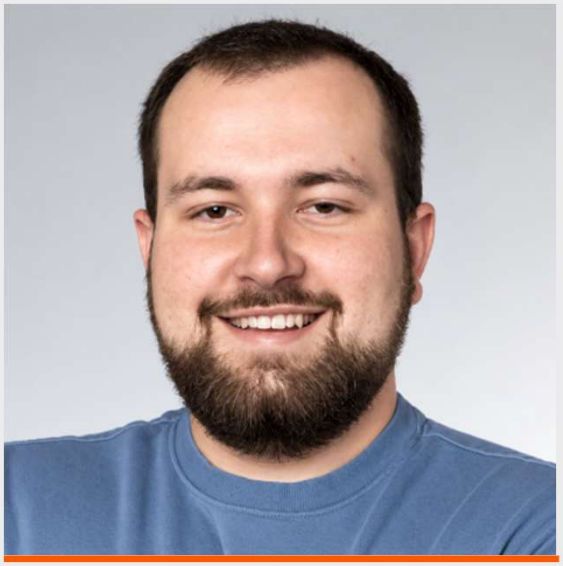
UNSERE HEUTIGEN REFERENTEN

first frame networkers



MARCO BORTOLUZZI

Systems Engineer Workplace



MIKA SCHÜRPF

Teamleiter Maintenance & Improvement

AGENDA

first frame networkers

- 11:00 Begrüssung & Vorstellung Referenten & SLKK?
- 11:05 Zahlen - Philippe Hirzel
- 11:10 Endpoints - Marco Bortoluzzi
- 11:25 Server - Mika Schürpf
- 11:40 Fragen & Antworten
- 11:45 Zusammenfassung & nächste Schritte

Fragen dürfen während der Präsentation mit der Chatfunktion gestellt werden

Das Webinar wird in Schweizerdeutsch gehalten

KURZVORSTELLUNG SLKK

first frame networkers

- Persönlich. Solidarisch. Verlässlich.
  - Schweizer Krankenkasse mit Sitz in Zürich
  - gegründet aus einer solidarischen Gemeinschaft
  - heute offen für alle Versicherten
  - persönliche und verantwortungsbewusste Betreuung
  - 32 Mitarbeiter



KURZVORSTELLUNG SLKK

first frame networkers

- Versicherungslösungen für jede Lebenslage
  - Grundversicherung (verschiedene Modelle)
  - Zusatzversicherungen
  - Spezialversicherungen
  - Partnerangebote
  - Gesundheitsförderung und Prävention



GESETZGEBUNG

first frame networkers

Datenschutzverordnung (DSV) - seit September 2023 in Kraft:

…Betriebssysteme und Anwendungssoftware stets auf dem neusten Sicherheitsstand gehalten und bekannte kritische Lücken geschlossen werden (Systemsicherheit)…

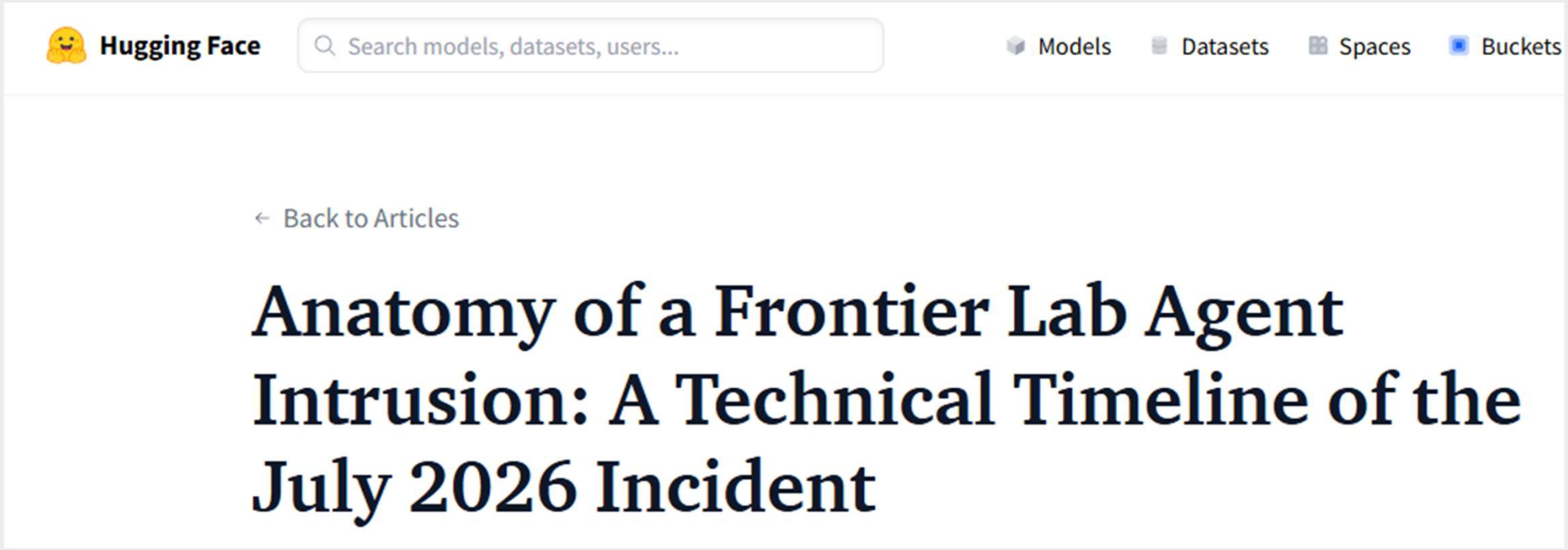
KI-ZEITALTER

first frame networkers

- «Bug-Apocalypse»
- «Patch-Apocalypse»
- KI findet Sicherheitslücken schneller als diese geschlossen werden
- Sicherheitslücken werden schneller geschlossen als Patches installiert
- Wie gehen wir damit um?

BEISPIELE

first frame networkers



BEISPIELE

first frame networkers

AI assistant hacks gym website in first known Australian autonomous cyber attack

By national AI reporter Cam Wilson and the Specialist Reporting Team's Rhiannon Hobbins

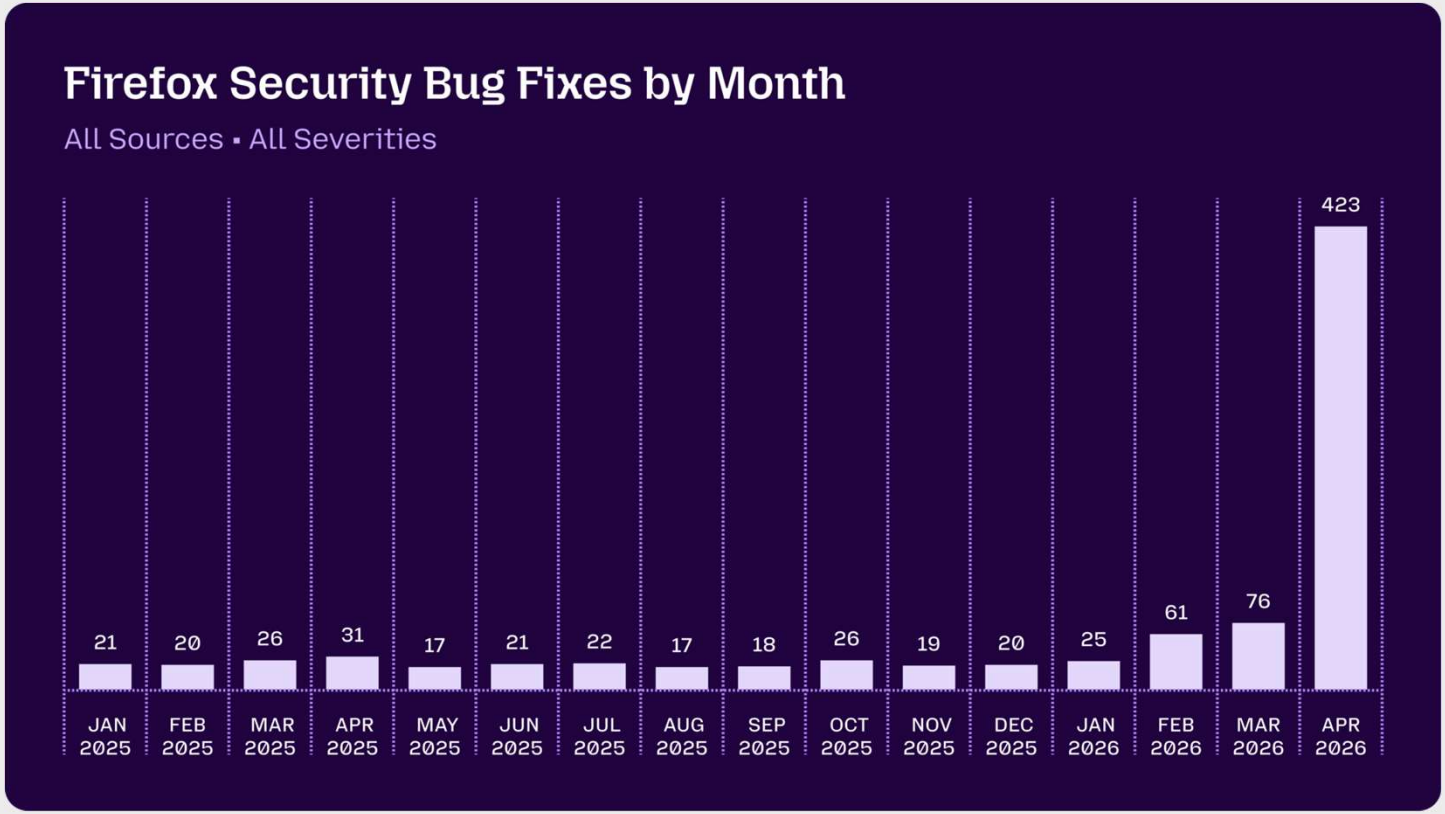
AI Ethics

Posted 9 Aug 2026 at 8:44pm, updated 10 Aug 2026 at 12:36am



MOZILLA FIREFOX

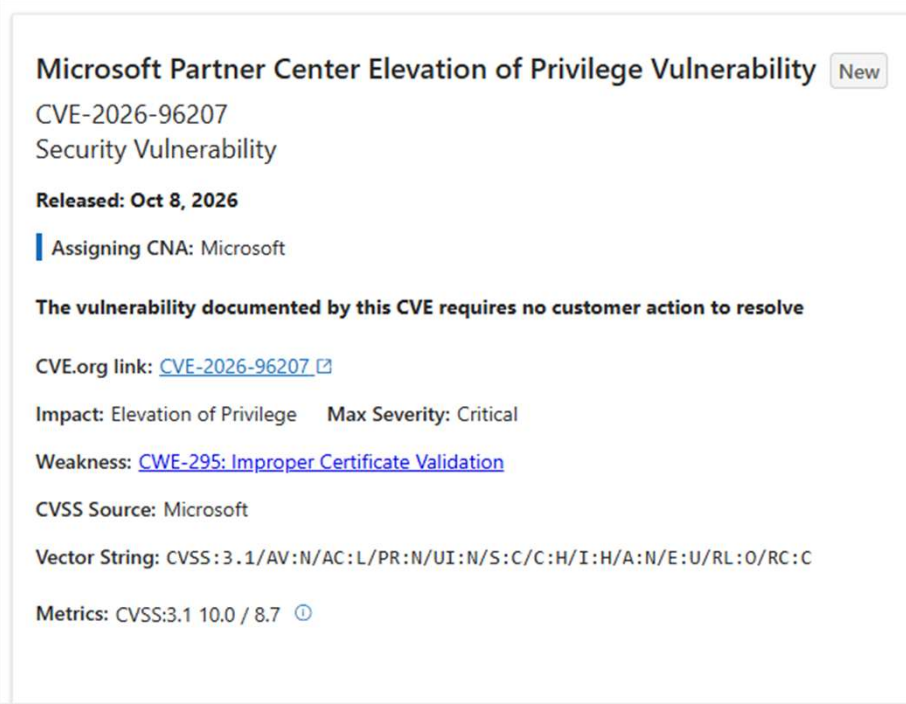
first frame networkers



CVE-2026-96207: MICROSOFT PARTNER CENTER ELEVATION OF PRIVILEGE

first frame networkers

ID	CVE-2026-96207
Schweregrad	10/10
Impact	Elevation of Privilege
Publicly disclosed	No
Exploited	No
Exploitability assessment	Less Likely



Microsoft Partner Center Elevation of Privilege Vulnerability New

CVE-2026-96207
Security Vulnerability

Released: Oct 8, 2026

Assigning CNA: Microsoft

The vulnerability documented by this CVE requires no customer action to resolve

CVE.org link: CVE-2026-96207

Impact: Elevation of Privilege Max Severity: Critical

Weakness: CWE-295: Improper Certificate Validation

CVSS Source: Microsoft

Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:N/E:U/RL:O/RC:C

Metrics: CVSS:3.1 10.0 / 8.7

SCHWACHSTELLEN BEWERTEN FRÜHER

first frame networkers

CVSS Score

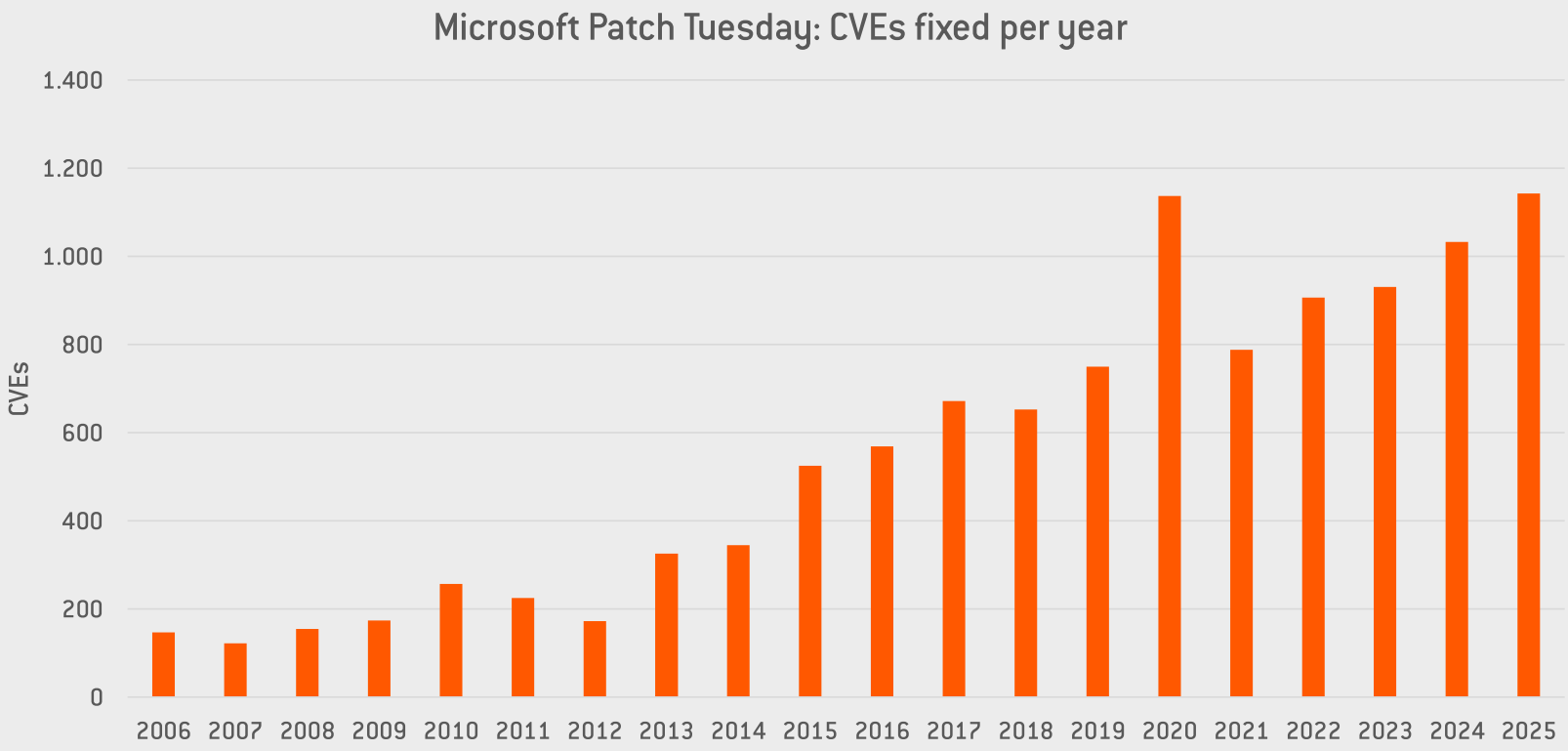
1/10

> 8.0 – aktiv tracken

< 8.0 –normal patchen

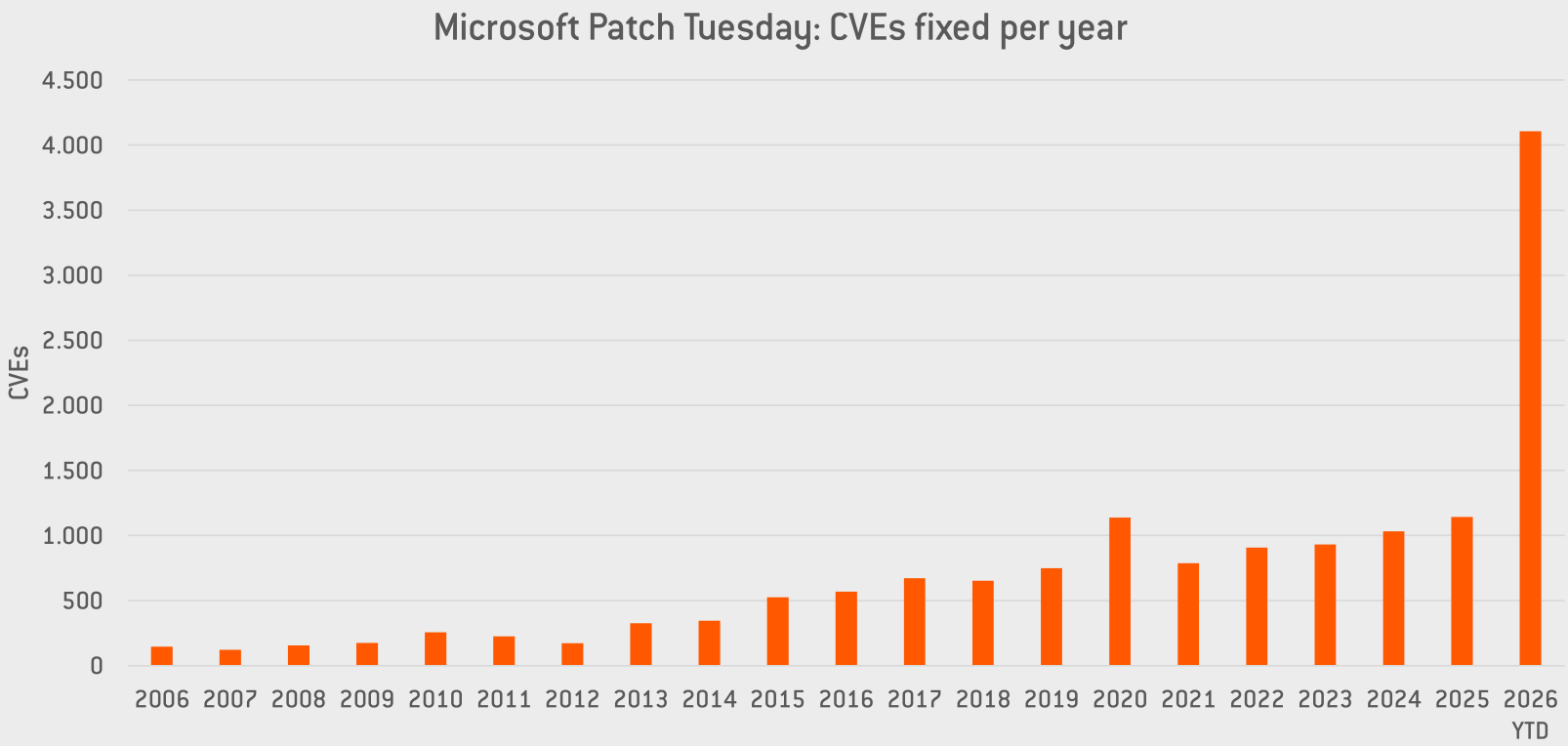
MICROSOFT PATCHES BIS 2025

first frame networkers



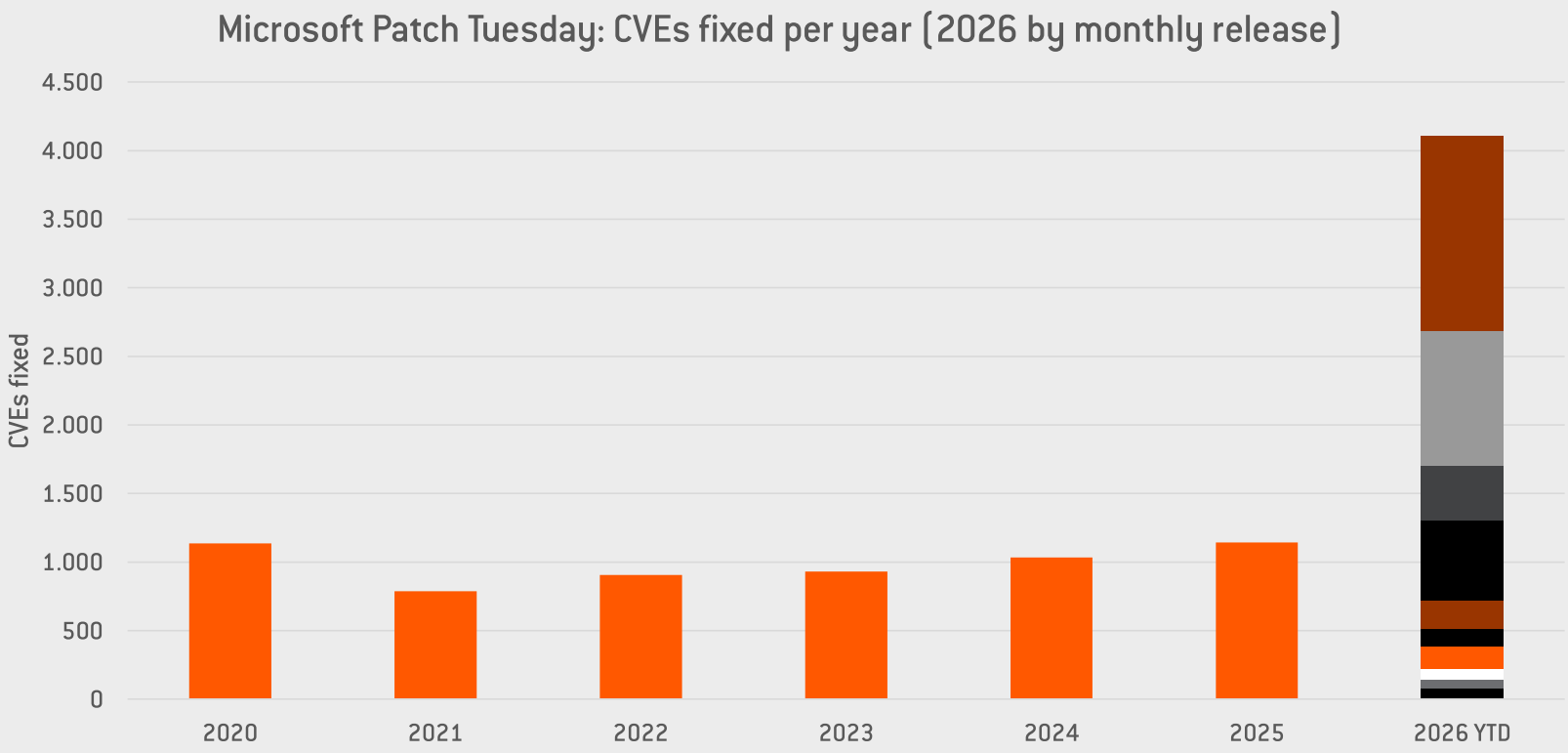
MICROSOFT PATCHES MIT 2026

first frame networkers



MICROSOFT PATCHES MIT 2026

first frame networkers



IST DAS ALLES RELEVANT?

first frame networkers

Philippe's monthly Report: Microsoft Patch Tuesday Juli 2026

Nachdem im Juni bereits ein neuer Rekord mit über 200 Patches aufgestellt wurde, sind es im Juli nun über 600 – ein Rekord in neuen Dimensionen. Durch den vermehrten Einsatz von KI zur Erkennung von Sicherheitslücken dürften diese Zahlen künftig weiter stark ansteigen. Dieses Phänomen wird allgemein als «Bug Apocalypse» bezeichnet, weil Administratoren in der Flut an Patches schlicht und einfach unterzugehen drohen.

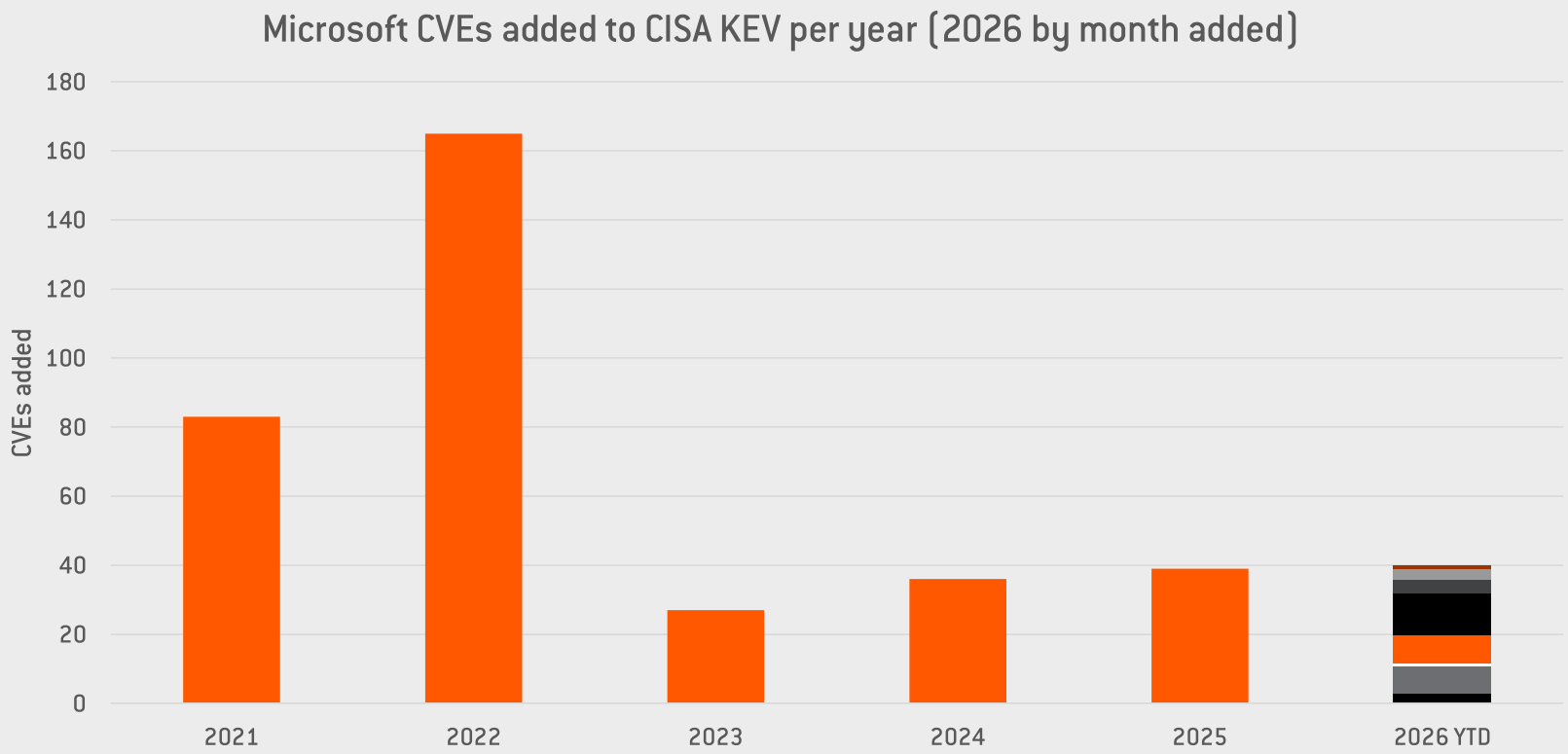


Mithilfe von KI können auch Schwachstellen behoben werden, deren Behebung sich bisher kaum gelohnt hat oder die in sehr alten Produkten vorkommen. Dieser Patch Tuesday zeigt dies exemplarisch anhand eines Patches für «Age of Empires II: Definitive Edition», ein 2019 veröffentlichtes Spiel, das wiederum ein Remaster des Originals aus dem Jahr 1999 ist.

Damit wird die korrekte Priorisierung von Updates noch wichtiger, um die eigenen Systeme weiterhin sicher betreiben zu können. Wir haben unsere Patch-Services wie «first endpoint update» deshalb weitestgehend automatisiert. Nur so lässt sich diese Flut an Patches effizient bewältigen.

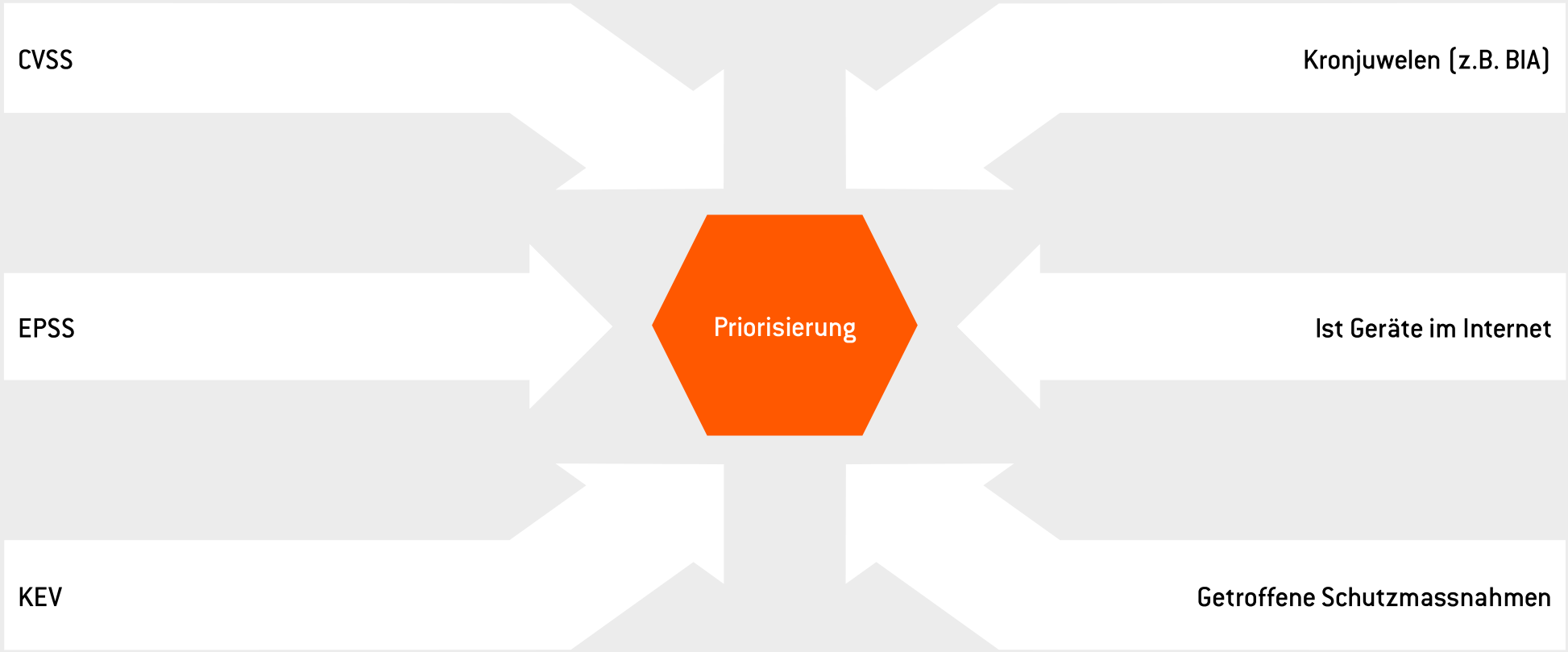
CISA KEV AM BEISPIEL MICROSOFT

first frame networkers



SCHWACHSTELLEN BEWERTEN JETZT

first frame networkers



BEISPIEL FÜR PRIORISIERUNG

first frame networkers

Angebot Referenzen Unternehmen Partner News + Blog Karriere Kontakt

first frame networkers

News

Startseite > News + Blog > News-Detail > Philippe's monthly Report: Microsoft Patch Tuesday September 2026

Mittwoch, 09. September 2026

Philippe's monthly Report: Microsoft Patch Tuesday September 2026

Microsoft hat diesen Monat knapp 1'000 Sicherheitslücken geschlossen. Dies sind mehr als im ganzen Jahr 2023. Wie letzten Monat bereits gesagt, müssen wir uns an diese Grössenordnung



Kundenportal

Support

ALPC oder Advanced Local Procedure Call klingt einerseits sehr wichtig, aber andererseits nicht sehr aussagekräftig. Es ist eine Komponente, mit welcher Prozesse auf einem Computer miteinander kommunizieren können. Diese Schwachstelle kann beispielsweise über manipulierte Word-Dateien ausgenutzt werden.

Erwähnenswerte Schwachstellen

Es sind mittlerweile zu viele Schwachstellen, um diese einzeln zu nennen – daher erwähnen wir aktuell betroffene Komponenten und nicht mehr einzelne Schwachstellen.

DNS

Im DNS-Server von Windows gibt es diverse RCE-Lücken. Diese erlauben es, einem DNS-Server eine manipulierte Netzwerkabfrage zu senden und danach beliebigen eigenen Code auf dem Server auszuführen. DNS-Server, welche direkt im Internet verfügbar sind, sollten schnell aktualisiert werden.

SQL

Im SQL-Server von Microsoft wurden diesen Monat auch diverse Sicherheitslücken repariert. Auch diese erlauben es, beliebigen Code auf dem SQL-Server auszuführen. Allerdings benötigen die meisten Sicherheitslücken einen am Server angemeldeten Benutzer, um ausgenutzt zu werden.

Exchange

Im Exchange gibt es vor allem eine Sicherheitslücke, die ich gerne ansprechen würde. Ein Angreifer kann auf dem Exchange Server beliebigen Code ausführen, sofern er vorher ein E-Mail mit einer angehängten Visio-Datei versendet hat.

Kritische Schwachstellen

Daneben behebt Microsoft zahlreiche weitere kritische Schwachstellen, unter anderem in Windows, Office, Azure und weiteren Produkten.

Statt sämtliche CVEs einzeln aufzuführen, verweisen wir für die technische Detailübersicht direkt auf den **Microsoft Security Update Guide**. Dort können die Sicherheitsupdates nach Produkt, Schweregrad und CVE gefiltert werden.

BEISPIEL FÜR SCHUTZMASSNAHMEN

first frame networkers

cyon

! my.cyon, Webmail und alle Hostings vorübergehend abgeschaltet

Das PHP-Projekt veröffentlicht heute, 21.10.2026 16:00, ein dringendes Sicherheitsupdate für kritische Sicherheits
Schutz deiner Websites und Daten haben wir um **15:45 Uhr** my.cyon, das Webmail, alle Webhostings, Managed S
Agencyserver sowie den Sitebuilder vorsorglich vom Netz genommen. Websites auf diesen Servern sind deshalb v
nicht erreichbar.

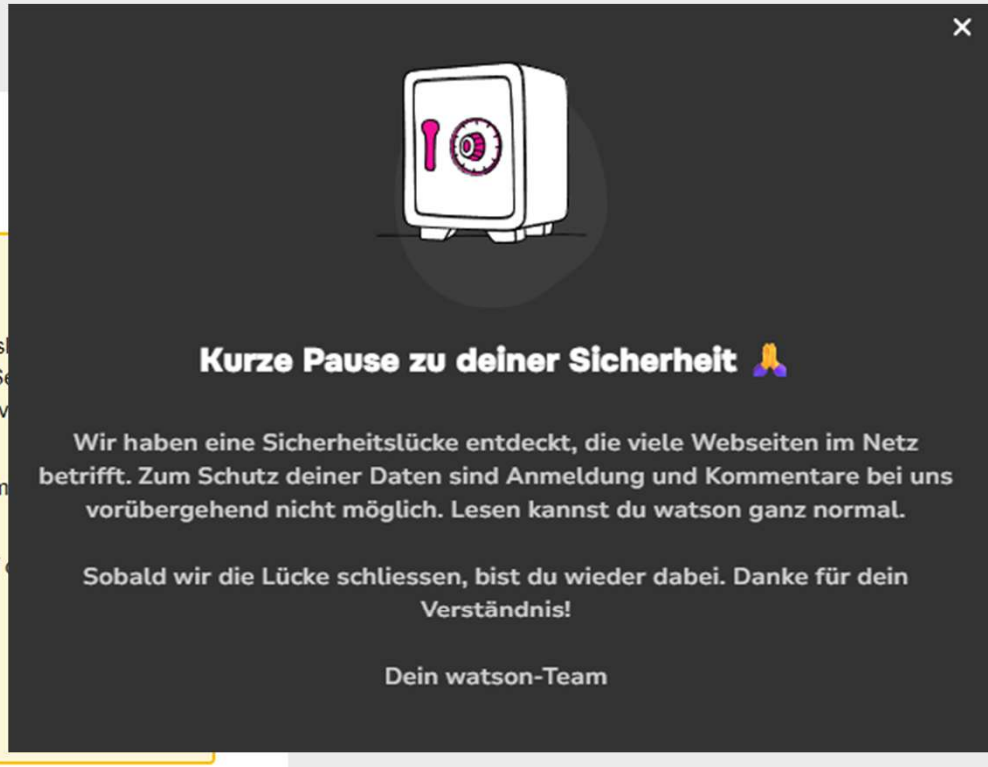
Der E-Mail-Verkehr ist davon nicht betroffen: Postfächer empfangen weiterhin E-Mails, und in E-Mail-Programm
Thunderbird, AppleMail, usw) lassen sich E-Mails wie gewohnt abrufen und versenden.

Sobald das Update eingespielt ist, schalten wir alle Dienste wieder ein. Neue Informationen veröffentlichen wir auf
auf status.cyon.info.

Details und alle Updates

Letztes Update: 21.10.2026, 15:45 Uhr

Einige Systeme sind beeinträchtigt



WAS KANN MAN MACHEN

first frame networkers

- Regelmässig Patchen – z.B. jeden Monat
- Priorisieren
- Patches vorziehen wo nötig
- Massnahmen ergreifen wo nötig

ENDPOINTS



FIRST ENDPOINT UPDATE

first frame networkers

Sicherheitsupdates mit Verantwortung für den Betrieb

Was FEU abdeckt

Windows und Microsoft-Anwendungen
Vereinbarte Drittanwendungen
Treiber und Firmware unterstützter Geräte

Was unser Team übernimmt

Updates nach Dringlichkeit bewerten
Verteilung und Ausnahmen steuern
Status prüfen und Probleme bearbeiten

KI erhöht das Tempo. Mehr Software und neue Schwachstellen halten den Patch-Druck hoch.

Ihr Nutzen: weniger eigener Aufwand für einen aktuellen Arbeitsplatz

TECHNOLOGIEN IM FEU-SERVICE

first frame networkers

Mehrere Technologien, ein betreuter Service

Microsoft Entra ID

Gerätegruppen und Zielgruppen

→

Microsoft Intune

Richtlinien und App-Verteilung

→

Notebooks und PCs

Verwaltete Arbeitsgeräte

Windows Update for Business

Windows, Treiber und Firmware

Patch My PC Cloud

Definierte Drittanwendungen in Intune

FEU verbindet die Werkzeuge mit Bewertung, Betrieb und Kontrolle

WINDOWS UND HARDWARE

first frame networkers

Für jede Update-Art der passende Weg

Windows	Sicherheits- und Qualitätsupdates über Windows Update
Microsoft-Anwendungen	Edge, Microsoft 365, Teams und OneDrive über Microsoft-Wege
Treiber und Firmware	BIOS / UEFI und Treiber über Windows Update for Business

Unterstützte Hardware gemäss Service-Dokumentation: HP, Lenovo und Microsoft.

Ihr Nutzen: Updates berücksichtigen auch die Basis unter Ihren Anwendungen

PATCH MY PC: APP-AUSWAHL

first frame networkers

Eine App-Bereitstellung beginnt mit dem passenden Umfang

01

Bestand erfassen

Discovery zeigt Apps
und vorhandene Versionen

02

Passende App wählen

Katalog, Variante und
Kundenbedarf abgleichen

03

Vorlage anwenden

Zielgruppen, Update-Ringe
und Verhalten festlegen

Update Only

Vorhandene App aktualisieren

Required

Verbindlich installieren

Available

Im Unternehmensportal anbieten

Ihr Nutzen: abgestimmte Anwendungen und wiederholbare Bereitstellung

PATCH MY PC: BEREITSTELLUNG

first frame networkers

Vom vorbereiteten Paket zur aktualisierten Anwendung

01

Patch My PC Cloud

Erstellt App-Paket und Regeln in Intune

02

Intune

Verteilt an die vorgesehenen Gruppen

03

Gerät

Prüft Voraussetzungen und installiert passend

04

Kontrolle

Meldet den Installationsstatus

Am Gerät arbeitet die Intune Management Extension. Update Only prüft die passende App-Variante.

Paket in Intune erstellt und App auf dem Gerät installiert sind zwei verschiedene Status.

Täglicher Abgleich und Update-Ringe halten Folgeversionen im geregelten Ablauf

PATCH MY PC: SICHERHEITSPRÜFUNGEN

first frame networkers

Mehrere Prüfschritte vor der Verteilung an Ihre Geräte

Quelle und Hash

Herstellerdatei und digitalen Fingerabdruck abgleichen

Signaturen

Katalog signiert
App-Signaturen prüfen, soweit vorhanden

Malware-Scan

VirusTotal
Bei grossen Dateien: Microsoft Defender

Pakettests

Neuinstallation, Update und Deinstallation prüfen

FEU ergänzt die Prüfungen durch Test- und Pilotgeräte in Ihrer Umgebung.

Die Kontrollen reduzieren Risiken. Sie garantieren keine vollständige Malwarefreiheit oder Kompatibilität.

Ihr Nutzen: geprüfte Paketbasis und kontrollierte Einführung im Arbeitsalltag

UPDATE-RINGE IM VERGLEICH

first frame networkers

Kleine Gruppen schaffen Zeit, Probleme zu erkennen

Update-Ringe	PreTest App-Vorprüfung	Test Erste Geräte	Pilot Alltag prüfen	Produktion Breit verteilen
Patch My PC	Tag 0	+1 Tag	+3 Tage	+7 Tage
Windows		+1 Tag	+3 Tage	+7 Tage

Standardwerte: Windows ab Veröffentlichung, Apps ab Deployment. Tatsächliche Installation kann später erfolgen.

SLKK als Praxisbeispiel: Test, Pilot und Produktion begrenzen den ersten Wirkungskreis

SCHLECHTE PATCHES ERKENNEN

first frame networkers

Installiert bedeutet noch nicht im Alltag bewährt

Technischer Status

Intune meldet Installation und Fehler.
FEU prüft den Windows- und BIOS-Stand.
Berichte zeigen Geräte mit Handlungsbedarf.

Rückmeldung aus Test und Pilot

Funktionieren wichtige Anwendungen?
Fallen Probleme nach dem Update auf?
Bei Auffälligkeiten: Verteilung prüfen.

Reporting im Hintergrund

first endpoint collector / Graph API, Power Automate, Dataverse und Power BI

Ihr Nutzen: Fehlende Updates und Störungen erhalten gezielte Aufmerksamkeit

DRINGENDE UPDATES VORZIEHEN

first frame networkers

Hohe Dringlichkeit erhält einen beschleunigten Weg

Normaler Zyklus	Bewerten	➡	Gestaffelt verteilen
Kritische Lücke	**SOC und Betrieb bewerten**	➡	**Gezielt vorziehen**

Windows: Expedite

Eine Intune-Richtlinie beschleunigt ausgewählte Qualitätsupdates.
Bei Apps steuern wir die Bereitstellung separat in Patch My PC / Intune.

Ihr Nutzen: weniger Wartezeit bei Lücken, die rasches Handeln erfordern

AUSNAHMEN UND ARBEITSALLTAG

first frame networkers

Rücksicht auf Geschäftssoftware und laufende Arbeit

Beispiel Java

Abhängigkeiten und Version abstimmen
Änderungen an kritischen Apps prüfen
Sonderfälle separat behandeln

Wenn Programme geöffnet sind

Patch My PC fordert zum Schliessen auf.
Begrenztes Verschieben hilft im Alltag.
Windows steuert Neustarts über Richtlinien.

Individuelle Geschäftsanwendungen sind separat zu vereinbaren und kein Standardumfang.

Ihr Nutzen: Schutz erhöhen und unnötige Unterbrechungen begrenzen

WINDOWS 11 UND FEATURE UPDATES

first frame networkers

Windows 11 braucht laufende Pflege und geplante Versionswechsel

Sicherheits- und Qualitätsupdates

Regelmässig Lücken schliessen
Zuverlässigkeit verbessern
Neustarts und Fristen steuern

Feature Updates unter Kontrolle

Unterstützte Zielversion festlegen
Wichtige Apps und Treiber prüfen
Zuerst Pilot, dann breiter ausrollen

FEU steuert die Einführung über Intune und behält den Supportzeitraum der Windows-11-Version im Blick.

Ihr Nutzen: ein aktuelles Windows 11 mit planbaren Veränderungen

WARUM PATCHEN UNVERZICHTBAR IST

first frame networkers

Auch ein funktionierender Computer kann verwundbar sein

Bekannte Lücken

Angreifer nutzen bekannte Schwachstellen gezielt aus

→

Geschäftsrisiken

Datenabfluss, Ransomware und Ausfälle können den Betrieb beeinträchtigen

→

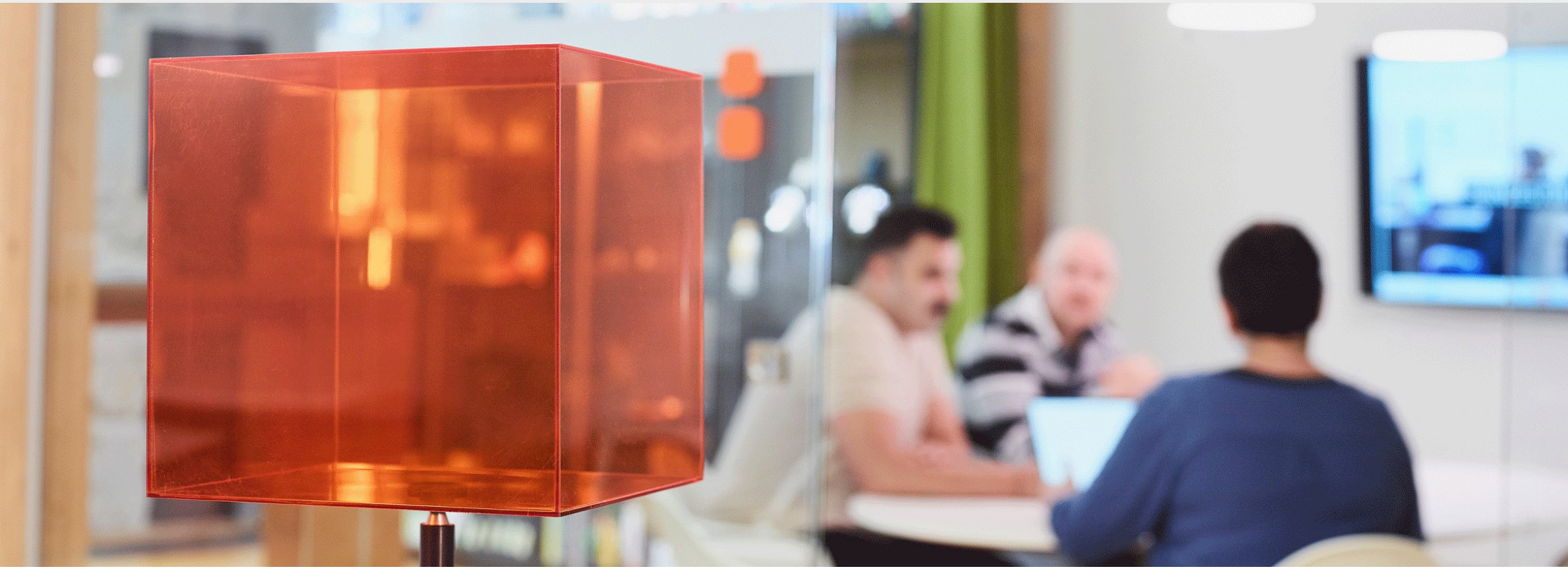
Regelmässig patchen

Sicherheitsupdates priorisieren, installieren und den Erfolg prüfen

first endpoint update verbindet zeitnahe Absicherung mit gestaffelter Einführung und Kontrolle.

Sicherheitspatches schliessen bekannte Lücken und reduzieren vermeidbare Risiken

SERVER



UNTERSCHIEDLICHE WARTUNGEN

first frame networkers

Kleine Serverwartung

12×

pro Jahr · monatlich

Regelmässig absichern

Sicherheitsupdates
des Betriebssystems

Meist geringes Änderungsrisiko
Üblicherweise keine Featureänderungen

Grosse Serverwartung

1×

pro Jahr

Das Fundament aktuell halten

Hosting & Infrastruktur
Storage, physische Server, Virtualisierung

Kernkomponenten
Exchange, Microsoft SQL, PostgreSQL, Veeam

Höheres Änderungsrisiko
Abhängigkeiten, Featureupdates, längere Ausfallzeiten

KLEINE SERVERWARTUNG

first frame networkers

Mehr als nur auf «Update» klicken



KLEINE SERVERWARTUNG

first frame networkers

01 **Analyse** → 02 **Beobachten / Testen** → 03 **Installation & Neustart** → 04 **Kontrolle** → 05 **Ausweisen**

Sicherheitsupdates prüfen

< 24 Stunden

Kontrolle nach dem Release

Handlungsbedarf klären

Dringend vorziehen
oder verschieben?
Welche Systeme betrifft es?

Kritische Systeme bewerten

Betroffene Systeme identifizieren
und Auswirkungen einschätzen

Philippe's Monthly Report

Die Analyse im Blog – empfohlen, um auf dem Laufenden zu bleiben.

KLEINE SERVERWARTUNG

first frame networkers

01 Analyse → 02 Beobachten / Testen → 03 Installation & Neustart → 04 Kontrolle → 05 Ausweisen



Täglich evaluieren

TÄGLICH

Bekannte Probleme prüfen
und neu bewerten

Bei bekannten Problemen →



Erweitert testen

BEI BEKANNTEN PROBLEMEN

Bekannte Probleme gezielt
mit erweitertem Testing untersuchen

KLEINE SERVERWARTUNG

first frame networkers

01 Analyse → 02 Beobachten / Testen → 03 Installation & Neustart → 04 Kontrolle → 05 Ausweisen

Vier Wartungstage pro Monat

3. Montag
Testsysteme
Ca. 1 Woche nach Release

4. Dienstag | **4. Donnerstag** | **4. Samstag**

Übrige Systeme gezielt verteilen
Ca. 2 Wochen nach Release

Risiken reduzieren · Abhängigkeiten berücksichtigen

Warum Server später als Clients?

Server sind Kernsysteme – ihr Ausfall kann viele Arbeitsplätze betreffen.

Sicherheit und Verlässlichkeit in Balance

KLEINE SERVERWARTUNG

first frame networkers

01 Analyse → 02 Beobachten / Testen → 03 Installation & Neustart → **04 Kontrolle** → 05 Ausweisen

Updates installiert & Neustart durchgeführt?



Kontrolle über mehrere Wege

Für ein verlässliches Ergebnis

Zusätzliche Kontrollen

Antivirenschutz

Managementsysteme

z. B. iLO oder vCenter

Gesundheit der Umgebung

Allgemeinen Zustand prüfen

KLEINE SERVERWARTUNG

first frame networkers

01 **Analyse** → 02 **Beobachten / Testen** → 03 **Installation & Neustart** → 04 **Kontrolle** → 05 **Ausweisen**

Monatlicher Report

AM 7. DES MONATS

Verfügbar per Mail
und im Kundensystem

Wartung transparent ausgewiesen

Installationen & Neustarts
Status auf einen Blick

Alle behandelten Systeme
Gesamtübersicht im Report

Künftig nur noch im Kundenportal

Noch kein Zugang als IT Manager?
Einfach bei unserem Service Desk (SD) anfragen.

GROSSE SERVERWARTUNG

first frame networkers

Stark verkürzte Darstellung

Deutlich umfangreicher als die kleine Serverwartung.
Individuell geplant – je nach Komponente und Kunde.

Vorbereitung & Planung

Neue Funktionen erhöhen die Fehleranfälligkeit.

Umfangreiche Vorbereitung vor der Umsetzung.

Über das Jahr verteilt

Hersteller veröffentlichen Updates zu unterschiedlichen Zeitpunkten.

Wartung zum passenden Zeitpunkt im Jahr.

Emergency Patches

Ungeplante Sicherheitsupdates erfordern direktes Handeln.

↑ Früher: **1–2** pro Jahr
Dieses Jahr: **5–6**

Unsere Empfehlung: Managed Server Full

Emergency Patches vollständig abgedeckt – ohne ungeplante Mehrkosten.

NEXT STEPS

first frame networkers

- Let's Talk!
  - Mit Ihrem Account Manager oder +41 41 768 08 00
  - Mit Mika Schürpf - Mika.Schuerpf@firstframe.net
  - Mit Marco Bortoluzzi - Marco.Bortoluzzi@firstframe.net
  - Mit Philippe Hirzel - philippe.hirzel@firstframe.net
- Weitere Infos
  - Detaillierte Information first endpoint update
  - Verschiedene Blog-Artikel zum Thema IT-Security

FEEDBACK-FORMULAR

first frame networkers



- Herzlichen Dank für Ihre Teilnahme am heutigen Webinar.
- Ihre Meinung ist uns sehr wichtig.
- Daher bitten wir Sie um eine Minute Ihrer wertvollen Zeit für die Feedbackumfrage.
- Unter allen ausgefüllten Fragebögen verlosen wir einen Bontique-Gutschein im Wert von CHF 75.—.
- Den Link finden Sie auch im Chat: https://forms.cloud.microsoft/e/BfMm3qgXS3

Herzlichen Dank

first frame networkers