CYBER SECURITY CLUSTER INTELLIGENCE BRIEF

Cyber Security Cluster · Ročník I · Číslo 7 · August 2026

Dátum vydania: 6. 9. 2026

Redakcia: Odborná rada Cyber Security Cluster

Šéfredaktorka: Ema Kopperová

Published Release

Publikované vydanie CYBSEC Executive Intelligence (2026-09-06). Distribúcia podľa klasifikácie TLP:GREEN.

AUGUST 2026: TRENDY KYBERNETICKEJ BEZPEČNOSTI A NOVÉ REGULAČNÉ RIZIKÁ

V TOMTO ČÍSLE

• Úvodník: August 2026 ukázal, že digitálne prostredie ostáva naďalej napäté a komplexné aj v letnom období.
• Udalosti mesiaca: 3 prípadov
• August 2026 v číslach
• Mýtus: Outsourcing kybernetickej bezpečnosti automaticky znamená vyššiu úroveň ochrany. Re
• RADAR: 6 úloh pre board · Regulatórny kompas

Úvodník šéfredaktora

August 2026 ukázal, že digitálne prostredie ostáva naďalej napäté a komplexné aj v letnom období. Aj v priebehu dovoleniek sa kybernetické hrozby nezastavujú a naopak – narástla intenzita útokov zameraných na menej pripravené organizácie. Popri útokoch ransomvérom a sofistikovanejších phishingových kampaniach sa čoraz viac diskutuje o pripravenosti na nové povinnosti vyplývajúce z menažmentu kybernetických rizík, ktoré vstúpia do platnosti v blízkej budúcnosti.

Panelová diskusia na tému prevádzkového riadenia kybernetickej pripravenosti, ktorá prebehla vo viacerých európskych metropolách, vyzdvihla význam systematickej spolupráce naprieč sektorovými hranicami. Organizácie, ktoré vnímajú kybernetickú bezpečnosť ako otázku riadenia a kultúry, budú schopné adaptovať sa rýchlejšie na meniace sa regulačné požiadavky i nové aktívne hrozby.

Našou odporúčanou stratégiou pre predstavenstvá a CEO na najbližšie obdobie je zintenzívnenie dialógu s risk manažmentom a IT oddeleniami, dôsledné vyhodnotenie aktuálnej pripravenosti na NIS2 a kritické prehodnotenie outsourcingu v oblasti kybernetickej bezpečnosti. Letné mesiace ponúkajú priestor pre revíziu procesov – odporúčame ho využiť na audit pripravenosti.

Ema Kopperová
CYBSEC / Executive Intelligence

Udalosť mesiaca (ukážka)

A. Globálny kontext — Medzinárodný útok ransomvérom na poskytovateľa telekomunikačných služieb ovplyvnil kontinuitu prevádzky

Prečo je to dôležité pre vás:

Všetky organizácie využívajúce outsourcing v oblasti digitálnych komunikačných služieb by mali zvážiť opätovné posúdenie zmluvných SLA a prevádzkových plánov obnovy, ako aj pripravenosť poskytovateľov na eskalované incidenty počas dovolenkových období.

Podrobnosti

Kedy	2026-08-19
Čo sa stalo	Dňa 19. augusta 2026 sa uskutočnil rozsiahly ransomvérový útok na významného poskytovateľa telekomunikačných služieb s dosahom na niekoľko krajín Strednej a Západnej Európy. Útočníci sa zamerali na infraštruktúru vysoke…
Dopad	Výpadok hlasových a dátových služieb, narušenie prevádzky v kritických sektoroch.
Skupina/Aktér	Nebola oficiálne identifikovaná konkrétna skupina.
RTO	Neuvedené v dostupných zdrojoch.
MTPD	16 hodín
Širší dopad	Reťazová reakcia na prevádzku služieb v zdravotníctve a doprave.

Finančný dopad: Neuvedené v dostupných zdrojoch.

Čo sa skutočne stalo

Dňa 19. augusta 2026 sa uskutočnil rozsiahly ransomvérový útok na významného poskytovateľa telekomunikačných služieb s dosahom na niekoľko krajín Strednej a Západnej Európy. Útočníci sa zamerali

na infraštruktúru vysokej dostupnosti, čo vyústilo do prerušenia niektorých hlasových a dátových služieb počas 16 hodín. Incident poukázal na prepojenosť digitálnych služieb a reálne prevádzkové riziká pre subjekty napojené na kritické komunikačné siete.

Komentár Odbornej rady — Ing. Rastislav Kopper, COO

Dopady útoku zasiahli nielen konečných zákazníkov, ale aj prevádzkovateľov verejných služieb, čo vyvolalo diskusiu o odolnosti dodávateľských reťazcov v sektore telekomunikácií a nutnosti posilniť monitoring kybernetických hrozieb aj počas letného obdobia s nižším personálnym obsadením.

Zdroj: ENISA — Ransomware attack affects telecom operator

Rada pre predstavenstvo:

Predstavenstvá by mali vyzvať k predloženiu aktualizovaných analýz dopadov na kontinuitu prevádzky v prípade výpadku outsourcingu a preveriť pokrytie incident response plánov v zmluvných vzťahoch s poskytovateľmi telekomunikačných služieb. Je vhodné zvážiť simuláciu obnovy procesov a overenie schopnosti internej komunikácie v prípade krízovej situácie.

Toto je len 1 z 3 udalostí mesiaca analyzovaných v plnej verzii. Plná verzia ďalej obsahuje „August 2026 v číslach“, odborný článok, plný RADAR a Regulatórny kompas.

Citát čísla

„Najväčšiu slabinu súčasných organizácií nepredstavuje technika, ale nedostatočná pripravenosť ľudí na sofistikované podvodné scenáre.“

— Dr. Martin Gregor, Vedúci analytik CERT.SK (CERT.SK — Správa o phishingových incidentoch v auguste 2026)

Číslo mesiaca

68

Percentuálny podiel spear-phishingu v rámci všetkých nahlásených phishingových incidentov v SR v auguste 2026

Zdroj: CERT.SK — Správa o phishingových incidentoch v auguste 2026

Ďalší krok pre vás

Toto číslo pripravilo Odborná rada Cyber Security Cluster ako Working Draft na redakčnú finalizáciu.

Ešte nie ste predplatiteľ

A1.2 predplatné

Pre prístup k ďalším analytickým materiálom kontaktujte CYBSEC na info.cybsec@pm.me

Máte predplatné IB

Kredit / členská zóna

Pripravte si interný reporting k odporúčaniam a zorganizujte strategický briefing na úrovni boardu.

Ste členom klastra

C2 · H1

Zúčastnite sa branžového fóra CYBSEC a požiadajte o hĺbkovú diskusiu k prioritným rizikám.

Preposlať kolegovi: Ak vám toto číslo prišlo užitočné, pošlite ho kolegovi v predstavenstve.

Cyber Security Cluster, z.z.p.o. · Skároš 331, 044 11 Skároš, Slovenská republika · IČO: 57743967
cybsec.center · media.cybsec@pm.me
© 2026 Cyber Security Cluster, z.z.p.o. Všetky práva vyhradené.
Ak si od Cyber Security Cluster Intelligence Brief neželáte ďalej dostávať, kontaktujte redakciu na media.cybsec@pm.me