Sprinx Systems, a.s.
Sídlo: Údolní 212/1, Praha 4
IČO: 26770211

V Praze, 30.3.2026

OFICIÁLNÍ VYJÁDŘENÍ KE KYBERNETICKÉMU INCIDENTU

V návaznosti na kybernetický incident ze dne 23. 3. 2026, o kterém jsme informovali naše zákazníky a příslušné orgány, tímto poskytujeme aktuální stav a vyjádření.

Klasifikace incidentu

- Útok byl směřován přímo proti společnosti Sprinx Systems,
- výpadek zákaznických služeb byl důsledkem preventivního vypnutí celé infrastruktury Sprinx Systems vč. služeb datového centra,
- žádná zákaznická data ani systémy nebyly identifikovány jako cíl jakýchkoliv škodlivých aktivit zjištěných v rámci incidentu.

Obnovení provozu

Všechny dotčené systémy a služby, byly:

- plně obnoveny,
- vráceny do provozního stavu,
- uvedeny do kontrolovaného a bezpečného režimu provozu.

Obnova proběhla standardními bezpečnými postupy.

Integrita dat a prostředí

Na základě provedené analýzy, dostupných logů a forenzního šetření:

- nebyl potvrzen žádný únik zákaznických dat či přístupových údajů z prostředí zákaznických systémů,
- nebyl potvrzení žádný podezřelý síťový provoz z/do zákaznických systémů.

Bezpečnostní stav systémů

Před opětovným uvedením do provozu byly všechny systémy:

- kompletně izolovány a analyzovány,
- znovu zprovozněny / obnoveny z bezpečných bodů,
- doplněny o dodatečná ochranná opatření.

Současný stav:

- systémy jsou plně funkční a bezpečné pro provoz,
- infrastruktura je monitorována ve zvýšeném režimu,
- bezpečnostní politiky (včetně DoS ochrany a přístupových kontrol) byly zpřísněny.

Soulad s regulatorními povinnostmi

Incident byl řešen v souladu s platnou legislativou:

- oznámení incidentu NÚKIB – 23.3.2026,
- oznámení incidentu PČR – 23.3.2026,
- aktivace interních bezpečnostních a krizových procesů,
- Sprinx Systems nadále plně spolupracuje s vyšetřujícími orgány.

Další kroky

V rámci posílení odolnosti jsme přijali a dále realizujeme:

- zpřísnění bezpečnostních politik a pravidel detekce,
- rozšíření monitoringu a reakčních scénářů,
- dodatečné ochranné vrstvy infrastruktury,
- průběžné bezpečnostní audity.

Závěrečné prohlášení

Kybernetický incident a následný výpadek poskytovaných služeb společností Sprinx Systems, a.s. byl způsobem protiprávním útokem třetí strany na společnost Sprinx Systems, a. s., nikoli selhání společnosti Sprinx Systems, a.s..

Důležité shrnutí:

- služby jsou plně obnoveny,
- systémy zákazníků jsou bezpečné a nedošlo k úniku zákaznických dat,
- infrastruktura je provozována ve stabilním a zabezpečeném režimu.

Důvěra a transparentnost

Bereme tento incident jako vážnou událost, která vedla k dalšímu posílení našich bezpečnostních standardů.

Naším cílem je dlouhodobě garantovat:

- dostupnost služeb,
- ochranu dat,
- transparentní komunikaci.

Jiří Jinger
bezpečnostní manažer
Sprinx Systems, a.s.

Jiří Jinger

Digitally signed by Jiří Jinger
Date: 2026.03.30 16:03:15 +02'00'