ALVAO automaticky hlásí kyber bezpečnostní incidenty NÚKIBu

13.10.2025 - Jiří Kocourek | PARCO Consulting s.r.o.

Společnost ALVAO ve svém softwarovém řešení nabízí firmám a organizacím možnost okamžitě reportovat kybernetické incidenty státním složkám. ALVAO nyní umožňuje automatizovaný reporting bezpečnostních incidentů přímo do Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB). Plánuje se i reporting pro Českou národní banku (ČNB). Tento přímý kanál přináší významné výhody: minimalizaci škod, úspory nákladů, které dle průzkumů mohou stát i malou firmu až 250.000 Kč na rychlou ochranu podnikání.

Kybernetické hrozby jsou stále sofistikovanější a firmy i veřejné organizace se s nimi setkávají čím dál častěji. Včasná reakce a rychlé nahlášení incidentu má přitom zásadní vliv na minimalizaci škod, ochranu citlivých dat a schopnost identifikovat útočníka. Česká společnost ALVAO proto do svého ITSM řešení pro organizace a firmy integrovala možnost automatizovaného reportingu incidentů přímo do Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB).

„Pokud organizace incident zaznamená a nahlásí ho okamžitě, lze zabránit dalším škodám a rychleji obnovit běžný provoz. Naopak zpoždění v reportování vede k vyšším finančním ztrátám, narušení důvěry zákazníků a někdy i k právním postihům,“ říká Petr Vitouch, IT Security manager ze společnosti ALVAO.

Úniky stojí peníze

Z britského vládního průzkumu „Cyber Security Breaches Survey 2025“ z letošního roku vyplynulo, že u firem, které v posledním roce řešily vážný kyber bezpečnostní incident, byl průměrný celkový náklad v přepočtu 230.000 korun, u středních a velkých firem činil dokonce 350.000 korun. Data jasně ukazují, že i „menší“ incidenty stojí reálné peníze – a že čas lidí je významná položka. Čím dřív je incident podchycen a koordinovaně řízen, tím méně času a externích výdajů se spálí.

Rychlý reporting kybernetických incidentů má několik klíčových přínosů. Kromě zabránění větším škodám a úspory nákladů, kdy minimalizujete náklady na obnovu systémů a dat, jde i o významný reputační příspěvek k udržení kredibility firmy a důvěry zákazníků.

Plnění legislativní normy a pomoc bezpečnostním složkám

Využití automatizovaného hlášení bezpečnostních incidentů s ALVAO napomáhá bezpečnostním složkám státu rychlé zachycení vystopování a eliminaci pachatele. Díky řešení ALVAO ale dosáhnete i nutného plnění legislativních povinností – s příchodem směrnice NIS2 jsou organizace povinny incidenty hlásit. Automatizace zajišťuje, že firmy povinnost splní bez prodlení. Výhodou je i

jednotná evidence incidentů – všechny události jsou zaznamenané na jednom místě, což usnadňuje audit a následnou analýzu.

ALVAO přitom nabízí nejen samotný reporting, ale i kompletní řízení procesů kolem bezpečnostních incidentů – od prvotního zachycení, přes kategorizaci, až po jejich vyřešení a dokumentaci. ALVAO systém disponuje vzorovým katalogem služeb pro bezpečnost (hlášení incidentů, řízení dodavatelů, hlášení spamu a phishingu) s potřebnými formuláři i procesy, takže si uživatelé nemusí nic vytvářet

sami. Systém se navíc dokáže integrovat i se standardními bezpečnostními monitoring systémy např. typu Zabbix či Lansweeper.

„Naším cílem je dát firmám do rukou nástroj, který jim pomůže nejen splnit povinnosti vůči NÚKIB, ale hlavně ochránit jejich podnikání. Automatizovaný reporting v ALVAO šetří čas, minimalizuje riziko lidské chyby a dává organizacím větší jistotu, že na hrozby zareagují včas,“ doplňuje Petr Vitouch
ze společnosti ALVAO.

Příprava hlášení pro ČNB

Celý systém je nastaven tak, že bezpečnostní aplikace pro reporting automaticky oznamuje bezpečnostní incidenty NÚKIBu a generuje XML sestavu v oficiálním formátu požadovaném NÚKIBem. Po schválení bezpečnostním manažerem jsou tato data automaticky odeslána NÚKIBu. *„Do budoucna plánujeme v rámci plnění evropského nařízení DORA, které je účinné od 17. ledna 2025, přímý reporting bezpečnostních incidentů pro Českou národní banku,“* dodává Petr Vitouch.

Evropské nařízení DORA (Digital Operational Resilience Act) je součástí strategie EU na posílení kybernetické odolnosti finančního sektoru. Cílem DORA je zajistit, aby finanční instituce měly robustní systémy, které dokážou odolat kybernetickým útokům, technickým poruchám a jiným digitálním hrozbám. Nařízením DORA se musí přizpůsobit finanční subjekty v EU, jako jsou banky, pojišťovny a investiční společnosti, a také jejich poskytovatelé ICT služeb, zejména kritičtí poskytovatelé. Evropská unie se implementací nařízení snaží zajistit jednotnost a vysoká pravidla pro řízení kybernetických rizik a odolnost celého finančního ekosystému.

O ALVAO

ALVAO je nástroj pro správu IT služeb (ITSM), který podněcuje efektivní práci, řád a přehledný systém ve vašich organizacích. Produkty Alvao jsou nejefektivnější, když jsou obě hlavní části použity dohromady, ale mohou být používány i jednotlivě.