



INCIDENT / VNITŘNÍ HLÁŠENÍ

Karta prvního hlášení incidentu

Pomůcka pro zaměstnance a koordinátora. Kontakty doplňte předem a uložte také mimo firemní e-mail.

1 / Přerušete podezřelou činnost

Nepokračujte v otevírání příloh, zadávání hesel ani potvrzování požadavků. Ozvěte se určenému internímu kontaktu jiným důvěryhodným kanálem.

2 / Popište fakta

Zapište čas zjištění, dotčený systém a přesné pozorování. Odlište, co jste viděli, od toho, co pouze předpokládáte. Neposílejte hesla ani přístupové tokeny.

3 / Zachovejte dostupné podklady

Poznamenejte znění chyby a dostupné identifikátory. Zprávu nemažte a podezřelý soubor dál nerozesílejte. Předání podkladů koordinujte s pověřenou osobou.

4 / Zásahy koordinuje odpovědná osoba

Neprovádějte improvizovanou obnovu nebo hromadné změny. O izolaci, vypnutí či restartu rozhoduje pověřený tým podle situace. U OT má přednost bezpečnost lidí a provozní pravidla.

5 / Určete další rozhodnutí

Koordinátor potvrdí převzetí, vlastníka řešení a další čas aktualizace. Ověří provozní dopad a zapojení dalších rolí. Externí oznamování a jeho lhůty se posuzují podle konkrétní situace.



PRACOVNÍ LIST

Vyplňte před incidentem

Vyplňte pro vlastní firmu. Do veřejných formulářů neposílejte citlivé údaje ani přístupové informace.

Interní koordinátor / telefon	
Zástupce / náhradní komunikační kanál	
IT nebo smluvní podpora / dostupnost	
Vlastník provozu / osoba pro komunikaci	
Při události: čas / systém / pozorování	

Otázky před uzavřením

Kdo převzal hlášení a kdy přijde další aktualizace?

Jaké zásahy byly schváleny a kdo je provedl?

Nacvičte předání informací při stolním cvičení TTX.

<https://www.cybersafety.cz/skoleni/#workshopy>

Autor pracovního materiálu: CyberSafety. Vlastní otázky a šablony pro interní práci. Rozsah přizpůsobte organizaci; nejde o potvrzení souladu s předpisy.