Incidens kezelés

Lépésről lépésre

Ha incidenst észlelsz, és nem tudod, mit tegyél, kövesd ezeket a lépéseket!

1. lépés: *Maradj nyugodt*! Még egy egészen apró kis incidens is mindenkit stresszes állapotba hoz. Ilyenkor a kommunikáció és az együttműködés nehézkessé válhat. De a nyugodtságod segít abban, hogy súlyos hibát ne kövess el. Különben is, a legtöbb incidens nem olyan, mint amilyennek első látásra tűnik.

2. lépés: *Vedd elő a jegyzeteidet!* Vegyél elő kézikönyvet! Nyisd ki az incidensek azonosításánál! Ezek után gondold végig a lényeges tennivalókat. Miközben ezt teszed, ne felejtkezz meg arról sem, hogy a feljegyzéseid bizonyítékként is szolgálhatnak. Válaszolj a négy kérdésre: *ki, mit, mikor, hol* és a további kettőre: *miért* és *hogyan*! Egy kis magnetofon hasznos lehet.

3. lépés: *Értesítsd a megfelelő embereket* és kérj segítséget! Szólj a biztonsági felelősnek és a főnöködnek! Kérd meg a munkatársaidat, hogy segítsenek az incidenskezelés folyamatában! Kérd meg a kollégáidat, hogy készítsenek pontos feljegyzést arról, hogy kivel beszélgetettek és partnereik mit mondtak! Ellenőrízd, hogy valóban azt teszik-e!

4. lépés: Juttasd érvényre azt az elvet, hogy *„csak az tudjon az incidensről, akinek tudnia kell”.* A lehető legkevesebb embert szólj az esetről. Emlékeztesd kollégáidat, hogy őket megbízhatóknak tartod, és ezért számítasz a diszkréciójukra. Kerüld a spekulációkat, kivéve ha éppen döntened kell, hogy mit tegyél. Nagyon gyakori, hogy az incidensről szóló kezdeti információ megtévesztő, és a kidolgozott munkatervedet menetközben el kell dobnod.

5. lépés: *Használj független kommunikációs eszközt!* Ha a számítógépeket érte az incidens, akkor az incidenskezelés során kerüld azt! Inkább telefont vagy faxot használj! Ne küldj az incidensről semmilyen információt elektronikus levélben, talk vagy chat formában, vagy news-on keresztül: az üzenetet a támadó elfoghatja és akár a helyzetedet is tovább ronthatja. Ha mégis számítógépet használsz, kódolj minden elektronikus levelet!

6. lépés: *Elemezd a helyzetet!* Tedd meg a szükséges lépéseket, nehogy a probléma súlyosabbá váljon! Általában ez azt jelenti, hogy a rendszert húzd le a hálózatról, bár a vezetőséggel való egyeztetés után az a döntés is születhet, hogy maradjon meg a kapcsolat, hogy a támadót elfoghassátok.

7. lépés: *Azonnal készíts másolatot az érintett rendszerről*, ha úgy véled, hogy incidens történt. Új médiát használj! Ha lehet, bináris vagy „bitről bitre” másolatot készíts.

8. lépés: *Véglegesen old meg a problémát!* Azonosítsd, mi ment tönkre, ha tudod. Javítsd ki azokat a hibákat, ami lehetővé tette az incidens bekövetkeztét.

9. lépés: *Állítsd vissza a normális menetet!* Miután ellenőrizted, hogy a korábbi mentésed még ép, incidens nyomai azon még nincsenek, állítsd vissza erről a rendszert és figyeld, hogy helyesen működik-e. Tanulj a tapasztalatokból, hogy legközelebb n(s)e érjen felkészületlenül en az incidens.