rent_a_CISO

NEGYEDÉVES JELENTÉS · VEZETŐSÉG ÉS INFORMATIKA

Minta Kft. · 2026. III. negyedév

MINTA. Kitalált cég és kitalált adatok. Így néz ki a jelentés, amelyet negyedévente kap az ügyvezető és az informatikai vezető.

Címzett	a Minta Kft. ügyvezetője
Másolatot kap	az informatikai vezető
Időszak	2026. július 1.–szeptember 30.
Biztonsági osztály	„jelentős”
Egyeztetve	az informatikai vezetővel, 2026. október 8-án
Készítette	Hornyák Sándor, megbízott információbiztonsági felelős

01 Röviden

Jó hírrel kezdem: a negyedévben nem volt bejelentendő incidens. Az informatikával közösen frissítettük a kockázatelemzést, a HR pedig megszervezte az éves oktatást, amelyen a munkatársak nagy része már részt vett.

Két dologban kérem a döntését: a távoli belépés kétlépcsős azonosításában és a mentések külső példányában. Mindkettőt az informatikai vezetővel együtt javasoljuk, ő is látta ezt a jelentést, és a megvalósítást is együtt tervezzük.

Az auditra való felkészültség 73%-on áll, tartjuk az ütemet.

TERÜLET	ÁLLAPOT	MEGJEGYZÉS
Incidenskezelés	[x] **Rendben**	Két esemény, mindkettőnél megvan a kiváltó ok
Dokumentáció	[x] **Rendben**	Szabályzat és kockázatelemzés frissítve
Oktatás	[~] **Folyamatban**	A HR szervezi, a munkatársak 81%-a teljesítette
Távoli hozzáférés	[!] **Döntést kér**	A VPN-belépéshez elég a jelszó
Mentés	[!] **Döntést kér**	Nincs a telephelytől független példány

> **Fontos tudni:** informatikai betörés és incidens ellen nincs biztos megoldás. Amit tehetünk, és amin dolgozunk: megnehezítjük a hackerek dolgát, és ha mégis baj van, gyorsan észrevesszük, és gyorsan helyreállunk.

02 A számok

MUTATÓ	II. NEGYEDÉV	III. NEGYEDÉV	CÉL
Bejelentett incidens	0	0	nincs cél
Kivizsgált biztonsági esemény	4	2	nincs cél
Oktatást teljesítő munkatársak	0%	81%	100% (dec. 31.)
Kritikus javítócsomagok átfutása	19 nap	9 nap	14 nap alatt
Sikeres visszaállítási teszt	0 / 1	2 / 2	negyedévente 1
Kétlépcsős azonosítás a felhőfiókokon	62%	94%	100%
Értékelt kulcsbeszállítók	2 / 9	6 / 9	9 / 9

03 Mi történt, és miért

Mindkét eseménynél elvégeztük a kiváltó ok elemzését (root cause analysis) az informatikával. Egyiket sem kellett bejelenteni.

Augusztus 12., adathalász e-mail

Mi történt	Három munkatárs kapott hamis számlaértesítőt. Egyikük rákattintott és megadta a jelszavát. A jelszót még aznap lecseréltük, a fiókban nem volt gyanús tevékenység.
Kiváltó ok	A levelezőrendszer nem jelölte a külső feladót, a munkatárs telefonról, sietve nyitotta meg a levelet. A fiókján még nem volt bekapcsolva a kétlépcsős azonosítás, ő a hiányzó 6% egyike volt.
Mit változtattunk	Az informatika bekapcsolta a „külső feladó” jelölést, és minden érintett fiókon a kétlépcsős azonosítást. A HR a szeptemberi oktatásba betette ezt az esetet, a tananyagot én adtam hozzá.

Szeptember 3., elveszett laptop

Mi történt	Egy munkatárs a vonaton hagyta a céges laptopját.
Kiváltó ok	Figyelmetlenség, folyamatbeli hiányt nem találtunk. A lemez titkosítva volt, az eszközleltár naprakész, 20 perc alatt távolról zároltuk. Illetéktelen nem fért hozzá adathoz.
Mit változtattunk	Nem kellett változtatni. Az eset megmutatta, hogy a titkosítás és a távoli zárolás a gyakorlatban is működik.

04 Mit kezdünk először

A sorrendet a kockázatelemzés adja, a cég kockázatkezelési eljárásrendjének skálájával: valószínűség (1–4) szorozva a hatással (1–4). 1–3 pont alacsony, 4–6 közepes, 8–9 magas, 12–16 kritikus. A pontokat az informatikai vezetővel együtt állítottuk be.

A jóváhagyott tűréshatár a közepes szint (legfeljebb 6 pont). Ami felette van, azt kezelni kell, vagy Ön dönt az elfogadásáról. A 4-es hatású kockázatról pontszámtól függetlenül Ön dönt.

KOCKÁZAT	VALÓSZÍN.	HATÁS	PONT	SZINT	TEENDŐ
Távoli belépés (VPN) csak jelszóval	3	4	12	KRITIKUS	kezelendő
Régi, már nem támogatott gyártási adatgyűjtő szerver	3	3	9	MAGAS	kezelendő
A mentések ugyanabban az épületben vannak, mint a szerverek	2	4	8	MAGAS	kezelendő, 4-es hatás
Három kulcsbeszállító értékelése hiányzik	2	3	6	közepes	tűréshatáron belül
A naplók csak az eszközökön vannak, 30 napig	3	2	6	közepes	tűréshatáron belül
Még nem volt incidensgyakorlat a vezetőséggel	2	2	4	közepes	tűréshatáron belül

05 Ami jól megy, és ahol fejlődhetünk

Ami jól megy

- A titkosítás és a távoli zárolás éles helyzetben is bevált.
- A kritikus javítócsomagok átfutása 19 napról 9 napra csökkent, ez az informatika munkája.
- A felhőfiókok 94%-án már van kétlépcsős azonosítás.

Ahol fejleszteni érdemes a rendszeren

- Központi naplógyűjtés: ma egy incidensnél eszközönként kell összeszedni a naplókat, és 30 nap után elvesznek.
- A régi gyártási szerver elkülönítése a hálózat többi részétől, hosszabb távon a kiváltása.
- Jogosultság-felülvizsgálat negyedévente az eddigi éves helyett, főleg a kilépők és a szerepkör-váltások miatt.
- Mentés: a külső példány után rendszeres visszaállítási teszt abból is.

06 Döntést kérek

1. **Kétlépcsős azonosítás a VPN-nél.** A meglévő licenc tartalmazza, külön költség nincs. Az átállás egy hétvégi délelőtt, ehhez kérem az időpont jóváhagyását. Az informatika végzi, én a tervezésben és a tesztben segítek.
2. **Külső mentési példány.** Becsült költség havi 60–90 ezer forint. Az informatikai vezető két ajánlatot kér be, kérem, hogy a decemberi költségvetésben hagyja jóvá.

07 Mi jön: ütemterv 2027 végéig

Negyedévekre bontva, a kockázati szint szerint. Mindenhol jelöltem, ki csinálja és mire van szükség hozzá. A változtatásokat az informatikával egyeztetve, az ő ütemezésükhöz igazítva csináljuk.

MIKOR	TEENDŐ	KI CSINÁLJA	MI KELL HOZZÁ	PRIOR.
2026 Q4	Kétlépcsős azonosítás a VPN-nél	informatika, én tervezek és tesztelek	egy hétvégi délelőtt	KRITIKUS
2026 Q4	Külső mentési példány, a mentési eljárás frissítése	informatika; az eljárást én írom	döntés, havi 60–90 e Ft	MAGAS
2026 Q4	Az oktatás lezárása	HR szervezi, a tananyagot én adom	egy pótalkalom, 1 óra	közepes
2027 Q1	A régi gyártási szerver elkülönítése	informatika, én ellenőrzöm	hálózati átalakítás, 1–2 nap	MAGAS
2027 Q1	Beszállítói értékelés lezárása	én, a beszerzéssel	három beszállító válasza	közepes
2027 Q1	Központi naplógyűjtés: igények, ajánlatok	közösen az informatikával	költségvetési keret 2027-re	közepes
2027 Q2	Negyedéves jogosultság-felülvizsgálat bevezetése	informatika, én ellenőrzöm	kb. 4 óra negyedévente	közepes
2027 Q2	AI-eszközök felmérése, felvétel a nyilvántartásba	én	rövid munkatársi kérdőív	közepes
2027 Q2	Asztali incidensgyakorlat a vezetőséggel	én vezetem	2 óra a vezetőség idejéből	közepes
2027 Q3	Belső próbaaudit	én, az érintett kollégákkal	1 nap, a kollégák ideje	MAGAS
2027 Q3	Visszaállítási teszt a külső mentésből	informatika, én dokumentálom	fél nap	MAGAS
2027 Q4	Éves kockázatelemzés-frissítés, terv 2028-ra	közösen az informatikával	két egyeztetés, 2–2 óra	közepes
2027 Q4	Központi naplógyűjtés bevezetése, ha a keret megvan	informatika, én a szabályokat írom	a Q1-es döntés alapján	közepes

08 Hol tartunk az auditig

TERÜLET	ÁLLAPOT
Nyilvántartás és osztályba sorolás	100%
Kockázatelemzés	90%
Oktatás	80%
Szabályzatok és eljárások	75%
Beszállítók	65%
Hozzáférés-kezelés	60%
Mentés és helyreállítás	40%

A két döntés után a mentés és a hozzáférés-kezelés ugrik a legtöbbet.

Ha bármelyik ponton kérdése van, hívjon nyugodtan. A következő jelentés előtt az informatikai vezetővel ismét átnézzük a számokat. A következő jelentés: 2027. január 15.

Hornyák Sándor
megbízott információbiztonsági felelős, Rent a CISO
info@rentaciso.hu · rentaciso.hu

rent-a-ciso