KPMG

COVID-19

Mit tegyen CIO és a CISO ebben a helyzetben?

2020. március

A COVID-19 járvány hatásai miatt egyre nagyobb az aggodalom, ami a vállalatokat is arra ösztönzi, hogy szervezetük megóvása érdekében mielőbb reagáljanak a kialakult helyzetre. A CIO és CISO szerepe ebben a helyzetben kiemelkedően fontos, hiszen kulcsszerepük van abban, hogy a vállalat a járvánnyal kapcsolatos korlátozások életbe lépte után is működni tudjon.

Tud-e az Ön vállalata hatékonyan működni távoli munkavégzéssel?

CIO/CISO-ként ehhez biztosítani kell, hogy a munkavállalók ismerjék a folyamatokat, és a munkavégzéshez szükséges eszközöket. Ehhez viszont szükség lehet arra, hogy felülvizsgálják a hozzáférési-, jogosultságadás- és kockázatkezelési folyamatokat.

Megfontolandó kérdések:

- Megtörtént-e a VPN koncentrátorok, portálok és gateway-ek átskálázása, hogy elbírja a megnövekedett terhelést, amit a jóval nagyobb számban távolról csatlakozó kollégák idéznek elő?
- Figyelembe vették-e azokat a kulcsszállítókat, alvállalkozókat és partnereket, akiknek szintén távolról kell csatlakozniuk, illetve az esetleges új kapcsolódási csatornákat, amelyeket a helyzet megkövetel?
- Tesztelték-e az infrastruktúrát a megnövekedett terhelésre?
- Előfordulnak-e nem hibatűrő elemek az infrastruktúrában, és van-e lehetőség ezek redundánssá tételére?
- Szükséges-e további távoli elérési jogosultságok, vagy hitelesítő adatok megadása a munkatársak számára?
- Rendelkezésre áll-e elegendő helpdesk kapacitás az esetlegesen megnövekedő belépési problémák, vagy a távoli eléréssel és munkavégzéssel kapcsolatos kérdések megválaszolására?
- Amennyiben a munkavállalóknak szükségük van további laptopokra a távoli munkavégzéshez, elérhetőek-e ezek a meglévő raktárkészletből, vagy rövid időn belül beszerezhetők-e, és van-e kapacitás a szükséges telepítések elvégzésére? Mi alapján priorizálja a vállalat az eszközök allokációját?
- Abban az esetben, ha az eszközök száma limitált, számításba vették-e, hogy alternatív elérést biztosítsanak a nélkülözhetetlen alkalmazásokhoz (pl. O365, OneDrive, belsőleg használt alkalmazások)?
- Számításba vették-e, hogy ez alatt az időszak alatt csak bizonyos alkalmazások legyenek elérhetőek, és a többi, nem nélkülözhetetlen alkalmazás blokkolva legyen?
- Korlátozza-e a vállalat bizonyos videó és audio telekonferencia-alkalmazások használatát, lehetséges-e, hogy ezt a korlátozást feloldják?
- Szükséges-e további felhőalapú konferencia és távmunka támogató megoldásokat beszerezni?
- Biztosítottak-e a munkavállalók számára a távmunkához szükséges belépési információk, elérhető-e a kapcsolódó oktatási anyag, szükség van-e további helpdesk kapacitás allokálására?

– Megoldható-e a helpdesk távolról való működtetése abban az esetben, ha a részleg összes munkatársának otthonról kell dolgoznia?
– Elérhetőek-e a munkatársak számára kézikönyvek, melyek az olyan alap helpdesk kérdéseket válaszolják meg, mint:
  » Hogyan lépjek be a rendszerbe?
  » Hogyan változtassam meg a jelszavamat?
  » Hogy érem el az alapszolgáltatásokat?
  » Hogy érem el a helpdesket?
  » Kik a kulcskontaktok krízis esetén?

Lehetséges-e a felmerülő új igények alapján az Önök digitális csatornáinak bővítése?

Az utazással kapcsolatos korlátozások és a vírus terjedése új igényeket támaszthat, és nagyobb forgalmat eredményezhet a vállalat digitális csatornáin.

Megfontolandó kérdések:

– Több felhasználó és ügyfél igényelheti a digitális csatornákon keresztül történő kapcsolattartást és munkavégzést, lehetséges-e ezen csatornák kapacitásának a növelése?
– Milyen módon monitorozza Ön a vállalata leterheltséget és a teljesítményt? Kinek a felelőssége dönteni a kihasználtsággal kapcsolatban, vagy prioritáslistát készíteni, ha a kihasználtság problémákat okoz?
– Meghatározták-e, mely szolgáltatásokat kell elrejteni, illetve milyen módon kell az ügyfelek számára elérhető folyamatokat korlátozni, ha a rendszer túlterhelt?
– Függ-e az Ön vállalata kulcsfontosságú call centerektől, és ha ezek nem elérhetőek, kapcsolatba léphetnek-e az ügyfelek Önökkel más csatornákon keresztül?
– Lehetséges-e, hogy a call center munkatásai távolról dolgozzanak, vagy hogy az egyes telephelyekre beérkező hívásokat átirányítsák más call centerekbe?
– Felülvizsgálták-e a call centerek és service/helpdeskek kommunikcáióját, és a kiszervezés lehetőségeit?
– Átbeszélték-e a kulcsszállítókkal a szerződésekben foglalt vállalásokat, és hogy miként fogják ezeket priorizálni a többi ügyfelüknek nyújtott szolgáltatásokkal szinkronban?

Függ az Ön vállalata kulcsfontosságú IT munkavállalóktól?

Előfordulhat, hogy a munkavállalók megbetegednek, vagy nem lesznek képesek eljutni a munkahelyükre, esetleg nem tudják elvégezni a munkájukat családi kötelezettségeik mellett. Emiatt a vállalatnak számolnia kell szignifikáns mértékű távolmaradással.

Megfontolandó kérdések:

– Mi történne, ha a kulcsfontosságú IT alkalmazottak (beleértve az alvállalkozókat) képtelenek lennének beutazni munkahelyükre vagy megfertőződnének a vírussal?
– Függ-e az Ön vállalata kulcsfontosságú feladatot betöltő munkavállalóktól? Hogy tudja lecsökkenteni ezt a függőséget, és biztosítani, hogy más munkatársak is hozzáférjenek a kritikus rendszerekhez?
– Megvizsgálta-e az IT biztonságért felelős csapat tagjainak feladatait és azonosította-e a kulcsszereplőket?
– Amennyiben a CISO nem lesz elérhető, ki lesz felelős a biztonsági intézkedések irányításáért és a kockázatkezelésért?

Mi a forgatókönyv az adatközponttal kapcsolatos zavarok elhárítására?

A vírus kihatással lehet az adatközpontra is. Ha az ott dolgozók közül bárkinek a vírus tesztje pozitív, az evakuációhoz és fertőtlenítéshez is vezethet, ami miatt napokra be kell zárni az adatközpontot.

Ezen túlmenően a közlekedés változásai nehezíthetik, esetenként ellehetetleníthetik a munkavállalók eljutását a munkahelyükre.

Megfontolandó kérdések:

– Rendelkezik-e az Ön vállalata katasztrófaelhárítási tervvel arra az eshetőségre, ha valamelyik adatközpontját evakuálni kell, illetve tesztelték-e ezt a tervet?
– Rendelkeznek-e másodlagos adatközponttal, és milyen gyorsan tudnak átkapcsolódni oda? Ki a felelős a folyamat levezényléséért?
– Függ-e az adattárház működtetése kulcsfontosságú munkavállalóktól (beleértve az alvállalkozókat), és hogy tudja Ön kezelni ezt a függőséget?

Képes-e az Önök vállalata átméretezni a rendelkezésre álló felhőtárhelyet?

Felmerülhetnek olyan új igények, amelyek a felhőalapú szolgáltatások kibővítéséhez vezetnek, ez pedig előre nem kalkulált költségnövekedést eredményezhet, de az is előfordulhat, hogy bizonyos szolgáltatások kihasználtsága csökken.

Megfontolandó kérdések:

- Képes-e az Ön vállalata monitorozni a felhőalapú szolgáltatások leterheltségét, és hatékonyan kezelni az erőforrások allokációját?
- Van-e már terve arra, hogy hogyan biztosítsák a többletköltségeket a felhőalapú szolgáltatások megfelelő támogatásához?

Függ-e szállítóktól az Ön vállalatának zavartalan működése?

A különböző szállítók szintén nyomás alá kerülhetnek, és a kialakult helyzet megzavarhatja az eddigi működésüket.

Megfontolandó kérdések:

- Azonosították-e a kritikus szállítókat, ideértve a kulcsfontosságú szolgáltatást nyújtó partnereket, és kidolgozták-e a tervet arra az esetre, ha leáll a működésük?
- Van-e stratégia arra vonatkozóan, hogy hogyan csökkentsék ezt a kialakult függőséget, beleértve a belső erőforrások használatát?
- Tárgyaltak-e a kulcsszállítókkal a megváltozott körülmények okozta új igényekről, és rendelkeznek-e a megfelelő elérhetőségekkel vészhelyzet esetére?
- Azonosították-e azokat az IT beszállítókat amelyek pénzügyi helyzete meginoghat, és kidolgozták-e a vészhelyzeti beszerzési stratégiát arra az esetre, ha ezek a szállítók csődbe mennek?

Mi történne biztonsági incidens esetén?

A bűnszervezetek arra használják a COVID-19 vírust, hogy célzott támadásokat intézzenek a vállalatokkal szemben, és hamis információkat tartalmazó weboldalakat hozzanak létre, ezzel növelve a kiberbiztonsági kockázatok bekövetkeztének esélyét.

Megfontolandó kérdések:

- Egyértelmű-e az Önök munkavállalói számára, hogy hol találhatják a legfrissebb COVID-19-cel kapcsolatos információkat és az ezekhez kapcsolódó intézkedéseket?
- Figyelmeztették-e a munkavállalókat arra az eshetőségre, hogy megnövekedhet az adathalász-támadások előfordulása?
- Amennyiben az Önök vállalata függ olyan rendszerektől és szolgáltatásoktól, mint a felhőalapú megoldások, rendelkeznek-e stratégiával az ide kapcsolódó biztonsági incidensekre kezelésére?
- Szükséges-e megváltoztatni a szervezet biztonságos működésre vonatkozó szabályait beleértve a kockázatos események monitorozását?

Mi történne IT incidens bekövetkezte esetén?

Miközben a világ a COVID-19-el van elfoglalva – az infrastruktúrával kapcsolatos megváltozott igények és felhasználói szokások, valamint az esetleges kibertámadások miatt – a vállalatnak számolnia kell az IT incidensek számának növekedésével.

Megfontolandó kérdések:

- Képes-e az Ön vállalata az incidensek távoli kezelésére, rendelkezésre állnak-e a szükséges kommunikációs eszközök, jogosultságok és folyamatok?
- Rendelkezésre áll-e egy virtuális war room arra az esetre, ha a fizikai elérés korlátozott?
- Függ-e az incidensek megoldása kulcsfontosságú munkavállalóktól, és ha igen, mit lehet tenni ennek a függőségnek a csökkentése érdekében?
- Miként változik a vészhelyzeti/incidensmanagement struktúra, ha a kulcs-incidensmanagerek/visszaállításért felelős munkatársak nem érhetőek el?
- Felkészültnek érzi-e a vállalatot a rendszeres és teljes háttérmentéseket illetően, és vissza tudják-e állítani a létfontosságú vállalati adatokat és rendszereket a legutolsó mentett állapotra, ha a legrosszabb szcenárió következik be?
- Hogyan kezelne egy sok rendszert/folyamatot érintő incidenst, miközben az ennek megoldására alkalmas munkavállalók távolról dolgoznak?

Megfelelően kihasználja a rendelkezésre álló erőforrásokat?

Elképzelhető, hogy az Ön részlegének lecsökkent számú munkavállalóval kell működnie, és emiatt át kell priorizálnia a beérkezett feladatokat.

Megfontolandó kérdések:

– Elvégezte-e a csapata feladatainak priorizálását, vannak-e olyan feladatok, amelyeket későbbre lehet halasztani, és amelyek helyett a csapata foglalkozhat az üzletmenet folytonosságtervezésével és a magas prioritású feladatokkal?

– Van-e lehetőségük olyan vészhelyzeti tartalékok lehívására, amelyek gyorsan fedezni tudják az eszközök beszerzését, illetve további alvállalkozók / specialisták felvételét?

– Felmérte-e, hogy melyik területek fontosak, és melyek azok, ahol csökkenteni lehet a felmerülő költségeken, ha kényszerű költségcsökkentést rendelnek el.

Megfelelő példát mutat Ön a munkavállalói számára?

Az egész vállalatra érvényes rendelkezéseken túl Öntől további útmutatást és támogatást várnak a kollégái.

Megfontolandó kérdések:

– Megbizonyosodott-e róla, hogy a csapata alkalmazza a szükséges higiéniai előírásokat beleértve a távoli munkavégzést?

– Rendelkezik-e a csapata eléréséhez szükséges naprakész kontaktadatokkal? Tisztában van-e a csapata azzal, hogy kit kell keresnie vészhelyzet esetén?

– Végiggondolta-e, milyen viselkedést vár el a csapatától?

– Mi történne, ha Ön cselekvőképtelenné válna, ki venné át az Ön szerepét?

Vigyázzon magára és sok szerencsét!

Amennyiben kérdése lenne, vagy további tanácsokra lenne szüksége, forduljon hozzánk bizalommal!

Kapcsolat:

Kórász Tamás
partner
IT tanácsadás
M: +36 70 333 1507
E: tamas.korasz@kpmg.hu

Lukács Kornél
igazgató
Kiberbiztonság
M: +36 70 977 6564
E: kornel.lukacs@kpmg.hu

Tillinkó Zsanett
szenior menedzser
CIO tanácsadás
M: +36 70 333 1586
E: zsanett.tillinko@kpmg.hu

KPMG.hu