enisa

EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG

Kiberbiztonsági útmutató kkv-k számára

12 LÉPÉS A VÁLLALKOZÁS BIZTONSÁGOSSÁ TÉTELÉHEZ

A Covid19 válság megmutatta, mennyire fontos az internet és általában véve a számítógépek a kkv-k számára. Ahhoz, hogy a vállalkozások a világjárvány idején is működjenek, számos kkv-nak olyan üzletmenet-folytonossági intézkedéseket kellett hoznia, mint például a felhőszolgáltatásokra való átállás, az internetszolgáltatásaik továbbfejlesztése, a honlapjaik frissítése és a távoli munkavégzés lehetővé tétele a munkatársaik számára.

Ez a tájékoztató 12 magas szintű gyakorlati lépést kínál a kkv-k számára arra vonatkozóan, hogy milyen módon tehetik biztonságosabbá rendszereiket és vállalkozásukat. Ez a kiadvány az ENISA részletesebb **„Cybersecurity for SMES – Challenges and Recommendations”**
(A kis- és középvállalkozások kiberbiztonsága - kihívások és ajánlások)
című jelentésének kísérője.

1 JÓ KIBERBIZTONSÁGI KULTÚRA KIALAKÍTÁSA

VEZETŐI FELELŐSSÉGEK KIJELÖLÉSE

A jó kiberbiztonság a kkv-k folyamatos sikerének kulcsfontosságú eleme. E kritikus funkció vonatkozásában a felelősséget a szervezeten belül egy olyan személyre kell ruházni, aki gondoskodik arról, hogy a kiberbiztonságra megfelelő erőforrásokat fordítsanak, ide értve a munkavállalók munkaidejét, kiberbiztonsági szoftverek, szolgáltatások és hardverek beszerzését, a személyzet képzését és hatékony szabályzatok kidolgozását.

A MUNKAVÁLLALÓI ELKÖTELEZETTSÉG ELÉRÉSE

A munkavállalók elkötelezettsége elérhető a vezetőség kiberbiztonságról szóló hatékony kommunikációjával, a kiberbiztonsági kezdeményezések vezetőség általi nyílt támogatásával, a munkavállalók számára megfelelő képzések tartásával, valamint a munkavállalók részére a kiberbiztonsági szabályzatokban meghatározottaknak megfelelő egyértelmű és konkrét szabályok megfogalmazásával.

KIBERBIZTONSÁGI SZABÁLYZATOK KIBOCSÁTÁSA

A kiberbiztonsági szabályzatokban egyértelmű és konkrét szabályokat kell meghatározni a munkavállalók számára arra vonatkozóan, hogy hogyan viselkedjenek a vállalat IKT-környezetének, berendezéseinek és szolgáltatásainak használata során. Ezeknek a szabályzatoknak ki kell emelniük annak a következményeit, ha a munkavállaló nem a szabályzatoknak megfelelően jár el. A szabályzatok felülvizsgálatát és aktualizálását rendszeresen el kell végezni.

KIBERBIZTONSÁGI ELLENŐRZÉSEK LEFOLYTATÁSA

A megfelelő ismeretekkel, készségekkel és tapasztalatokkal rendelkező személyeknek rendszeres ellenőrzéseket kell lefolytatniuk. Az ellenőrök legyenek függetlenek, akár külső vállalkozók, akár a kkv-n belüli személyek, és a napi informatikai műveletektől függetlenül végezzék tevékenységüket.

ADATVÉDELMI EMLÉKEZTETŐ

Az EU általános adatvédelmi rendelete[1] értelmében minden olyan kkv-nak, amely az EU/EGT lakosainak személyes adatait kezeli vagy tárolja, gondoskodnia kell arról, hogy az adatok védelme érdekében megfelelő biztonsági ellenőrzéseket alkalmazzon. Ez magában foglalja annak biztosítását, hogy a kkv nevében eljáró harmadik feleknél megfelelő biztonsági intézkedések legyenek érvényben.

[1] Általános adatvédelmi rendelet
https://ec.europa.eu/info/law/law-topic/data-protection_hu

2

MEGFELELŐ KÉPZÉSEK NYÚJTÁSA

Rendszeres kiberbiztonsági tudatossági képzéseket kell biztosítani minden munkavállaló számára annak érdekében, hogy képesek legyenek a különböző kiberbiztonsági fenyegetések felismerésére és kezelésére. Ezeket a képzéseket a kkv-kra kell szabni, és a valós életben felmerülő helyzetekre kell összpontosítaniuk.

Speciális kiberbiztonsági képzést kell tartani a vállalkozáson belül a kiberbiztonságért felelős személyek számára annak érdekében, hogy rendelkezzenek a munkájuk elvégzéséhez szükséges készségekkel és kompetenciákkal.

3

HARMADIK FELEK HATÉKONY KEZELÉSE

Gondoskodni kell minden szállító, különösen az érzékeny adatokhoz és/vagy rendszerekhez hozzáféréssel rendelkezők aktív kezeléséről, és arról, hogy azok teljesítsék az elfogadott biztonsági szinteket. Szerződéses megállapodásokkal kell szabályozni azt, hogy a szállítók milyen módon tegyenek eleget e biztonsági követelményeknek.

4

INCIDENS-REAGÁLÁSI TERV KIALAKÍTÁSA

Készítsen világos útmutatást, feladatokat és felelősségi köröket tartalmazó hivatalos, dokumentált incidens-reagálási tervet annak érdekében, hogy minden biztonsági incidensre időben, szakszerűen és megfelelő módon reagáljanak. A biztonsági fenyegetésekre történő gyors reagálás érdekében mérlegelje olyan eszközök igénybe vételét, amelyek a rendszert nyomon követik és gyanús tevékenység vagy a biztonság megsértése esetén riasztanak.

5

A RENDSZEREKHEZ VALÓ BIZTONSÁGOS HOZZÁFÉRÉS

Bátorítson mindenkit arra, hogy használjon legalább három véletlenszerű, általános szóból mondattá kombinált „jelszó-kifejezést", amely a megjegyezhetőség és a biztonság nagyon jó kombinációját jelenti. Ha egy tipikus jelszót választ:

- Az legyen hosszú, tartalmazzon kis - és nagybetűket, esetleg számokat és speciális karaktereket is.
- Kerülje a nyilvánvaló szavakat, például „jelszó", illetve az olyan betű- vagy számsorokat, mint például az „abc", vagy az „123".
- Ne használjon online megtalálható személyes adatokat.

Valamint, akár jelszavakat, akár jelszó-kifejezéseket használ,

- Azokat ne használja máshol is.
- Ne ossza meg azokat a kollégáival.
- Vezessen be többlépcsős hitelesítést.
- Használjon dedikált jelszókezelőt.

6

AZ ESZKÖZÖK BIZTONSÁGOSSÁ TÉTELE

A munkavállalók által használt eszközök, például asztali számítógépek, laptopok, táblagépek vagy okostelefonok biztonságának elérése a kiberbiztonsági program egyik kulcsfontosságú intézkedése.

A SZOFTVEREK FRISSÍTÉSEIT ÉS HIBAJAVÍTÁSAIT MINDIG TÖLTSE LE.

Ideális esetben egy központosított platformot használjon a javítások kezelésére. A kkv-k számára erősen ajánlott:

- Valamennyi szoftverük rendszeres frissítése.
- Az automatikus frissítések bekapcsolása, amennyiben lehetséges.
- A manuális frissítést igénylő szoftverek és hardverek beazonosítása.
- Mobil és IoT eszközök figyelembe vétele.

VÍRUSVÉDELEM

Egy központilag kezelt vírusvédelmi megoldást minden eszköztípuson be kell vezetni és a folyamatos hatékonysága érdekében naprakészen kell tartani. Ne telepítsen kalózszoftvereket sem, mivel azok rosszindulatú szoftvereket tartalmazhatnak.

EMAIL- ÉS WEBES VÉDELMI ESZKÖZÖK ALKALMAZÁSA

Vegyen igénybe olyan megoldásokat, amelyek blokkolják a spam e-maileket, a rosszindulatú weboldalakra mutató linkeket tartalmazó e-maileket, a rosszindulatú csatolmányokat, például vírusokat tartalmazó e-maileket és az adathalász e-maileket.

TITKOSÍTÁS

Az adatokat védje azok titkosításával. A kkv-knak gondoskodniuk kell a mobil eszközökön, például laptopokon, okostelefonokon és táblagépeken tárolt adatok titkosításáról. A nyilvános hálózatokon, például szállodai vagy repülőtéri WiFi hálózatokon keresztül továbbított adatok esetében gondoskodni kell az adatok titkosításáról, akár virtuális magánhálózat (VPN) alkalmazásával, akár a weboldalakhoz SSL/TLS protokollt használó biztonságos kapcsolatokon keresztül történő hozzáféréssel. Gondoskodni kell arról, hogy a saját webhelyek megfelelő titkosítási technológiát alkalmazzanak az ügyfelek adatainak az interneten történő továbbítás alatti védelme érdekében.

7 A HÁLÓZAT BIZTONSÁGOSSÁG TÉTELE

MOBILESZKÖZ-KEZELÉS MEGVALÓSÍTÁSA

A távmunka lehetővé tétele során sok kkv engedélyezi a munkavállalók számára saját laptopok, táblagépek és/vagy okostelefonok használatát. Ez számos biztonsági aggályt vet fel az ezeken az eszközökön tárolt érzékeny üzleti adatok vonatkozásában. A kockázat kezelésének egyik módja egy mobileszköz-kezelési (MDM) megoldás alkalmazása, amely a kkv-k számára lehetővé teszi, hogy:

- Meghatározzák, mely eszközök férhetnek hozzá a rendszereikhez és szolgáltatásaikhoz.
- Ellenőrizzék, hogy az eszközre telepítették-e a legfrissebb vírusvédelmi szoftvert.
- Meghatározzák, hogy az eszköz titkosítva van -e.
- Megerősítsék, hogy az eszközre telepítették-e a legfrissebb szoftverjavításokat.
- Biztosítsák az eszköz PIN-kóddal és/vagy jelszóval való védelmét.
- Távolról töröljék az eszközről a kkv adatait, ha az eszköz tulajdonosa az eszköz elvesztését vagy ellopását jelentené, vagy ha az eszköz tulajdonosának a kkv-nál fennálló munkaviszonya megszűnik.

TŰZFALAK HASZNÁLATA

A tűzfalak kezelik a hálózatba belépő és onnan kilépő forgalmat, és a kkv-k rendszereinek védelme szempontjából kritikus eszközöknek számítanak. Valamennyi kritikus rendszer védelme érdekében tűzfalakat kell telepíteni, különösen a kkv-k hálózatának az internettel szembeni védelmében kell tűzfalat alkalmazni.

TÁVOLI HOZZÁFÉRÉSI MEGOLDÁSOK ELLENŐRZÉSE

A kkv-knak rendszeresen ellenőrizniük kell a távoli hozzáférési eszközöket, hogy azok biztonságosak legyenek, különösen:

- Minden távoli hozzáférési szoftverre biztosítani kell a javítócsomagok és frissítések letöltését.
- A gyanús földrajzi helyekről vagy bizonyos IP-címekről történő távoli hozzáférést korlátozni kell.
- A munkavállalók távoli hozzáférését kizárólag a munkájukhoz szükséges rendszerekre és számítógépekre kell korlátozni.
- A távoli hozzáféréshez biztosítani kell az erős jelszavak alkalmazását és ahol lehetséges, a többtényezős hitelesítés bevezetését.
- A feltételezett támadásokra vagy szokatlan gyanús tevékenységekre való figyelmeztetés érdekében biztosítani kell a felügyelet és a riasztás aktiválását.

8 A FIZIKAI BIZTONSÁG JAVÍTÁSA

Megfelelő fizikai ellenőrzéseket kell alkalmazni mindenütt, ahol fontos információkat tárolnak. A vállalati laptopot vagy okostelefont például nem szabad az autó hátsó ülésén felügyelet nélkül hagyni. Ha egy felhasználó elmegy a számítógéptől, azt mindig le kell zárnia. Egyébként az automatikus zárás funkciót minden üzleti célra használt eszközön be kell kapcsolni. Az érzékeny nyomtatott dokumentumokat szintén nem szabad felügyelet nélkül hagyni, és amikor azokat nem használják, biztonságosan el kell tárolni.

9 BIZTONSÁGI MENTÉSEK BIZTONSÁGA

A kulcsfontosságú információk helyreállításának lehetővé tétele érdekében biztonsági mentéseket kell készíteni, mivel ezek hatékony módot jelentenek, például egy zsarolóvírus-támadáshoz hasonló katasztrófa utáni helyreállításra. A következő biztonsági mentési szabályokat kell alkalmazni:

- a biztonsági mentés rendszeres és lehetőség szerint automatizált,
- a biztonsági mentést a kkv termelési környezetétől elkülönítve kell tárolni,
- a biztonsági mentések legyenek titkosítva, különösen, ha azokat a helyszínek között mozgatják,
- a biztonsági másolatokból történő rendszeres adat - visszaállítás képességét le kell tesztelni. Ideális esetben a teljes visszaállítást az elejétől a végéig rendszeresen le kell tesztelni.

10

A FELHŐ HASZNÁLATA

Bár a felhőalapú megoldások számos előnyt nyújtanak, bizonyos egyedi kockázatokat hordoznak, amelyeket a kkv-knak a felhőszolgáltatókkal való szerződéskötés előtt mérlegelniük kell. Az ENISA közzétette a „Felhőbiztonsági útmutató kkv-k számára”[2] című kiadványt, amelyet a kkv-knak a felhőre való áttéréskor figyelembe kell venniük.

A felhőszolgáltató kiválasztásakor a kkv-knak meg kell győződniük arról, hogy az nem sérti a törvényeket, illetve a rendeleteket azáltal, hogy az adatokat, különösen a személyes adatokat az EU/EGT-n kívül tárolja. Az EU általános adatvédelmi rendelete például előírja, hogy az EU/EGT-n belüli lakosok személyes adatait csak nagyon speciális feltételek mellett szabad az EU/EGT-n kívül tárolni vagy továbbítani.

2 https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes

11 BIZTONSÁGOS ONLINE WEBHELYEK

Elengedhetetlen, hogy a kkv-k biztosítsák online weboldalaik biztonságos konfigurálását és fenntartását, valamint a személyes adatok, illetve pénzügyi adatok, például a hitelkártyaadatok megfelelő védelmét. Ez magába foglalja a weboldalak rendszeres biztonsági tesztelését a lehetséges biztonsági hiányosságok azonosítása érdekében, valamint rendszeres felülvizsgálatok lefolytatását a weboldalak megfelelő karbantartása és frissítése céljából.

12 INFORMÁCIÓ KERESÉSE ÉS MEGOSZTÁSA

A számítógépes bűnözés elleni küzdelem hatékony eszköze az információ megosztása. A számítógépes bűnözéshez kapcsolódó információk megosztása a kkv-k számára kulcsfontosságú, hogy jobban megértsék az őket fenyegető kockázatokat. Azok a cégek, amelyek a hasonló vállalatoktól hallanak a kiberbiztonsági kihívásokról és azok leküzdéséről, nagyobb valószínűséggel tesznek lépéseket rendszereik biztonsága érdekében, mintha az ilyen részleteket iparági jelentésekből vagy kiberbiztonsági felmérésekből hallanák.

EURÓPAI UNIÓS KIBERBIZTONSÁGI ÜGYNÖKSÉG

AZ ENISA-RÓL

Az Európai Uniós Kiberbiztonsági Ügynökség (ENISA) az Unió azon ügynöksége, amelynek célja az Európa-szerte egységesen magas szintű kiberbiztonság megvalósítása. A 2004-ben létrehozott és az uniós kiberbiztonsági jogszabály által megerősített Európai Uniós Kiberbiztonsági Ügynökség hozzájárul az uniós kiberpolitikához, kiberbiztonsági tanúsítási rendszerek alkalmazásával javítja az IKT-termékek, -szolgáltatások és -folyamatok megbízhatóságát, együttműködik a tagállamokkal és az uniós szervekkel, és segíti Európát abban, hogy felkészüljön a jövő kiberbiztonsági kihívásaira. A tudásmegosztás, a kapacitásépítés és a figyelemfelkeltés révén az Ügynökség a legfontosabb érdekelt felekkel együtt arra törekszik, hogy megerősítse az összekapcsolt gazdaságba vetett bizalmat, fokozza az uniós infrastruktúra ellenálló-képességét és végső soron megőrizze Európa társadalmának és polgárainak digitális biztonságát. Bővebb információért lásd: www.enisa.europa.eu

ENISA
Európai Uniós Kiberbiztonsági Ügynökség

Athéni iroda
Ethnikis Antistaseos 72 &
Agamemnonos 14,
Chalandri 15231, Attiki,
Görögország

Irákliói iroda
95 Nikolaou Plastira
700 13 Vassilika Vouton,
Heraklion, Görögország

enisa.europa.eu