A Kaspersky működése a jelenlegi politikai helyzetben

2022. február 28.

Kedves Partnereink!

Mindannyian figyelemmel kísérjük az Ukrajnában és környékén zajló eseményeket. Kihívásokkal teli és bizonytalan időszak ez. Társaságunk számára továbbra is kiemelt fontosságú partnereinkkel és ügyfeleinkkel szembeni kötelezettségeink teljesítése.

A Kaspersky üzleti tevékenysége továbbra is stabil lábakon áll, technológiai és működési folyamatai pedig erősek, és alkalmazkodnak a kialakult helyzethez. Feladatunk, hogy ügyfeleinket megvédjük a kibertámadásokkal szemben, legyenek bármely országban is, ez alól a jelenlegi politikai helyzet sem kivétel. Biztosítani szeretnénk Önt, hogy cégünk továbbra is garantálja vállalt kötelezettségeinek teljesítését, beleértve a termékek és frissítések zavartalan elérhetőségét, valamint a pénzügyi tranzakciók folyamatosságát. A Kaspersky egy nemzetközi magáncég, vállalkozásainkat helyi szervezetek irányítják, mely lehetővé teszi, hogy hatékonyan ellenőrizhessük nemzetközi és helyi tevékenységeinket egyaránt. **Helyi szervezeteink 2008 óta pénzügyi önállóságot élveznek, és a partnerkapcsolataikat is közvetlenül kezelik.** Ezáltal a regionális partnerekkel folytatott üzleti tranzakcióink és számlázásaink helyi szervezeteken és helyi bankokon keresztül történnek.

2017 óta vállalatunk jelentős intézkedéseket vezetett be **a nagyobb átláthatóság, továbbá megoldásaink megbízhatóságának növelése érdekében.** Ezek közé tartozik az adatfeldolgozó rendszerünk áthelyezése Svájcba az európai, egyesült államokbeli, kanadai és több ázsiai-csendes-óceáni ország felhasználói számára. A Zürichben található adatközpontok, ahol a fenyegetésekkel kapcsolatos adatokat dolgozzuk fel, világszínvonalú létesítmények és teljes mértékben megfelelnek az iparági szabványoknak. Megosztott infrastruktúránk, beleértve a Kaspersky Security Network szervereit is, a világ különböző országaiban találhatók a nagyobb működési sebesség és rugalmasság érdekében. **Adatszolgáltatásunk, továbbá mérnöki**

gyakorlatunk biztonságát és integritását független, harmadik felek által végzett értékelések igazolják: a Big Four auditor által végzett SOC 2 Audit, valamint az ISO 27001 tanúsítvány és a TÜV Austria által nemrégiben ismételten kiadott tanúsítvány. Mindezen harmadik féltől származó dokumentumok kérésre rendelkezésre állnak.

A globális vezetőség kiemelt figyelemmel kíséri a jelenlegi helyzetet, és készen áll az azonnali intézkedésre. Különös tekintettel a konfliktusövezetben jelentett új kibertámadásokra, termékeinket frissítettük, így olyan egyedi technológiákat láttuk el őket, amelyek védelmet nyújtanak a káros, rosszindulatú programokkal szemben. Ügyfeleink továbbra is védettek: nem észleltünk sikeres kibertámadásokat közöttük.

A jelenlegi helyzet valószínűleg a kiberfenyegetések számának növekedéséhez vezet majd. **Ügyfeleink támogatása érdekében ingyenes hozzáférést biztosítunk CTI (Cyber Threat Intelligence) portfóliónkhoz, beleértve a fenyegetésekkel kapcsolatos jelentéseket (Threat Report), a fenyegetések felkutatását (Threat Lookup) és a Cloud Sandbox szolgáltatásunkat is.** Ezt a hozzáférést kezdetben egy hónapig biztosítjuk, ami, ha a helyzet úgy kívánja, tovább hosszabbítható. Kérjük vegye fel a kapcsolatot hivatalos viszonteladó partnerével annak érdekében, hogy a megfelelő módon élhessen ezzel a lehetőséggel.

Kétségtelen, hogy ez egy kihívásokkal teli időszak mindannyiunk számára. Reméljük, Ön továbbra is biztonságban lesz ebben a kritikus időszakban, és ami a kiberfenyegetéseket illeti, ránk számíthat: mi továbbra is garantáljuk ügyfeleink biztonságát.

Üdvözlettel,

Eugene Kaspersky