BEZPEČNOST V DOBĚ KRIZE

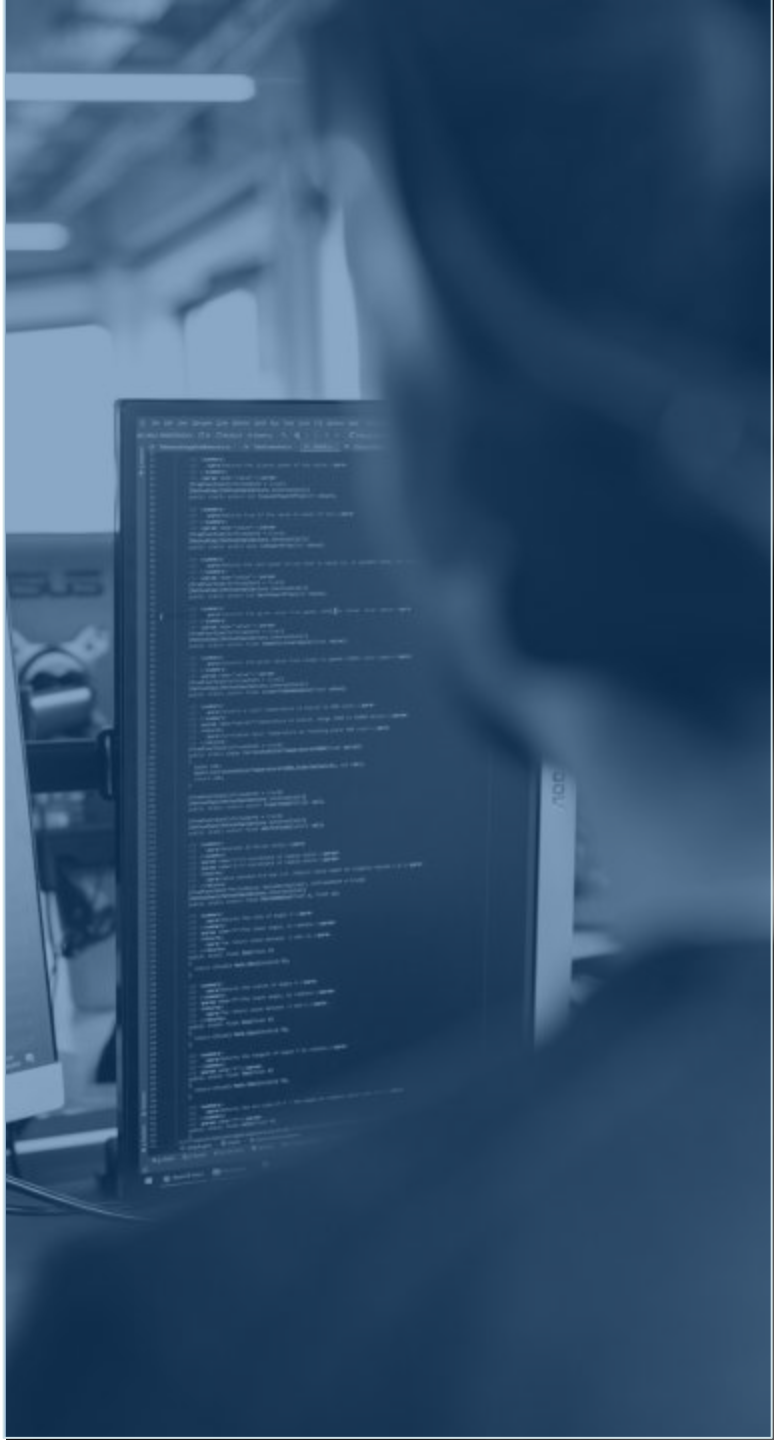
March, 2022

Powered by CYBEREADY

Proč na tom záleží

Kybernetická aktivita v souvislosti s rusko-ukrajinským konfliktem prudce narůstá, a přestože nejsme do konfliktu přímo zapojeni, týká se nás všech.

Každá světová krize má svůj kybernetický rozměr a prudký nárůst počtu phishingových e-mailů ukazuje, že tato krize není v ničem jiná.



Co se děje

1 Obě strany na sebe navzájem podnikly kybernetické útoky, které zahrnují malware pro vymazání dat a vyřazení webových stránek z provozu, aby se zabránilo jejich legitimnímu používání.

2 Tyto útoky se ne vždy podaří zastavit a často infikují zařízení a webové stránky, jež nejsou do konfliktu zapojeny. To zahrnuje také vaše firemní a osobní zařízení.

3 Vaše osobní účty na sociálních sítích jsou také ohroženy hackerským útokem za účelem šíření nepravdivých informací nebo malwaru.

Co můžete udělat pro ochranu své domácí sítě

Nainstalujte aktualizace operačního systému a zabezpečení. Pokud jsou k dispozici, mělo by se na počítači nebo v telefonu zobrazit oznámení.

Přidejte druhý faktor pro ověření svých účtů na sociálních sítích (Facebook, LinkedIn, Twitter atd.) a e-mailových účtů. Pokud je to možné, přidejte také záložní e-mailový účet.

Informujte vaše přátele a rodinu o tom, co se děje, a vyzvěte je, aby udělali totéž.

Co můžete udělat pro ochranu naší sítě

O vnitřní zabezpečení sítě se staráme my, takže nemusíte dělat nic technického.

V tomto období může docházet k většímu počtu phishingových útoků. Dávejte pozor na e-maily požadující vaši asistenci v technických nebo finančních věcech.

Vždy kontrolujte e-mailovou adresu odesílatele – nezapomeňte, že jde o nejdůležitější krok při odhalování phishingu.