Časté dotazy o službě ALEF Octoshield

1) Proč je obrana proti kybernetickým hrozbám kritickou oblastí pro každou společnost bez ohledu na její velikost?

Analytické zprávy společností Gartner a Forbes naznačují, že rok 2021 byl rekordní vysokým počtem narušení IT bezpečnosti a kybernetických útoků. Týká se to jak běžných uživatelů, tak malých podniků až po velké společnosti, nemocnic a vládních organizací – cílem kybernetických zločinců je každý.

2) Mám na svém firemním počítači nainstalovaný antivirus, používám bezpečnostní funkce zabudované v operačním systému počítače a při přístupu k firemním zdrojům používám dvoufázové ověření, to nestačí?

Vzhledem k tomu, že kybernetické útoky jsou stále sofistikovanější a kyberzločinci je snáze zahajují, vaše současná bezpečnostní opatření nemusí stačit. Nástroje a postupy kybernetické bezpečnosti je proto třeba neustále monitorovat a aktualizovat, aby bylo možné reagovat na nové hrozby. Pro společnost bez vysoce specializovaných odborníků na IT bezpečnost je těžké udržet krok.

Je třeba si uvědomit, že tradiční antivirová řešení spoléhají na detekci virů na základě tzv. signatur, tj. hledají v souborech konkrétně popsané znaky známých hrozeb. A i když některé antiviry nabízejí i tzv. heuristickou analýzu, která se snaží předpovídat potenciální hrozby zpětnou analýzou chování softwaru ve vašem počítači, jedná se stále jen o základní vrstvu ochrany, která v současné době nemusí být dostatečná vzhledem k prudkému vývoji malware.

3) Hodně jsme investovali do ochrany našeho centrálního IT před kybernetickými útoky. Proč to nestačí a měli bychom rozšířit i ochranu osobních počítačů?

Dlouhotrvající pandemie COVID donutila řadu lidí pracovat z domova přes své internetové připojení a tím se jejich firemní počítač stal ještě více klíčovou součástí celkové bezpečnosti firmy. Tento počítač není používán pouze pro firemní účely, ale i pro osobní potřeby, kdy lidé přes něj přistupují na různý obsah na internetu, který může být velmi nebezpečný. Je tedy mnohem více vystavený bezpečnostním rizikům, než pokud by byl používaný pouze ve firmě a připojený do její interní IT sítě. Proto si zaslouží větší míru ochrany před kybernetickými útoky, než může poskytnout běžný antivirový systém.

4) Všechno to zní složitě, kde mám vůbec začít s budováním kybernetické ochrany?

I když vybudování týmu kybernetické bezpečnosti a implementace nezbytných bezpečnostních řešení může trvat několik měsíců a bude to znamenat i značné investice, vaše kybernetická bezpečnost vám může být poskytnuta jako služba. Stejně jako si předplatíte software jako je Office 365 nebo služby jako Netflix, můžete od nás získat kybernetickou bezpečnost pro své počítače, tj. službu OctoShield, za měsíční poplatek.

5) Jak dlouho trvá spuštění služby OctoShield? A co zaměstnanci pracující na home-office?

Službu kybernetické bezpečnosti OctoShield nasadíme během 1 až 5 dnů v závislosti na velikosti vaší organizace. Služba se vztahuje na zaměstnance pracující ve vaší kanceláři nebo doma pomocí notebooků nebo chytrých telefonů. Máme to pro vás připravené.

6) Co přesně dostanu ve službě OctoShield?

Za měsíční poplatek za každé chráněné zařízení, který odpovídá zhruba ceně tří šálků kávy, získáte řadu následujících funkcí kybernetické bezpečnosti:

• nepřetržitou ochranu před různými typy škodlivého softwaru, který se snaží útočníci nepozorovaně nainstalovat do vašeho počítače

• nepřetržitý dohled a blokování komunikace z vašeho počítače na nebezpečné internetové domény a webovské stránky, ještě předtím, než bude z nich váš počítač infikovaný škodlivým softwarem

• pošleme vám upozornění na to, že došlo k podezřelé události nebo bezpečnostnímu útoku na váš počítač a případně vám s jejich odstraněním pomůžeme

Naše řešení je založeno na produktech Cisco Systems, přední společnosti v oblasti kybernetické bezpečnosti, která spolupracuje s nejrenomovanějšími společnostmi a organizacemi po celém světě. Cisco Systems ve své databázi sbírá on-line informace o bezpečnostních hrozbách a útocích z miliónů svých zařízení na celém světě.

7) Co se stane, když budu napadený kybernetickým útokem?

OctoShield ochrání váš počítač za všech okolností díky technologiím Cisco Systems. Ty automaticky zastaví kybernetický útok nebo výrazně sníží jeho dopad na vaše zařízení. Naši specialisté vám následně pošlou informace o tom, co se stalo, aby vám vysvětlili příčiny a následky útoku. Pokud se rozhodnete využívat službu OctoShield PLUS, pak pro vás zpracují forenzní analýzu a pomůžou s odstraněním bezpečnostních zranitelností, díky nimž k útoku došlo.

ALEF NULA a.s. I Pernerova 691/42, 186 00 Praha 8, Česká republika
Telefon: +420 225 090 240 | Fax: +420 225 090 112
cz-reception@alef.com | www.alefnula.com