

Objednáváme u Vás služby bezpečnosti sítě v následujícím rozsahu:

Služby budou poskytovány nejen v režimu průběžných "preventivních" činností, ale i v režimu "reakcí" na konkrétní události.

Jedná se o následující služby a činnosti:

**A. Kontrola definovaných bezpečnostních pravidel a souvisejících procesů a postupů:**

A.1. Preventivní činnost:

A.1.1. kontrola bezpečnostních pravidel systémů bezpečnostní infrastruktury

A.1.2. kontrola stavu (aktualizací) firmwaru

A.1.3. sledování událostí, logů na systémech,

A.2. průběžný security audit logů, v případě potřeby i v jednotlivých zařízeních (použití SIEM, korelace,

agregace, vyhodnocování a uchovávání)

A.3. Reakce na události:

A.3.1. včasná detekce úspěšných i neúspěšných pokusů o narušení bezpečnosti,

A.3.2. analýza rizik,

A.3.3. vyhodnocení rizik,

A.3.4. úprava příslušné metodiky (poučení z incidentu) pro další následnou pravidelnou preventivní činnost

A.3.5. provedení případných konfiguračních změn na dotčených systémech

**B. Účast na změnovém řízení, zejména doporučení při změně pravidel a konfigurace:**

B.1. Schvalování bezpečnostních pravidel, konfigurací a jejich změn.

B.2. Součinnost se subjektem zajišťujícím systémovou integraci, součinnost s auditory a dalšími relevantními orgány dle potřeb Objednatele.

**C. Kontrola a návrhy řešení bezpečnostních incidentů a postupů jak jim předcházet:**

C.1. zpracování dokumentace - postupů pro zvládání vzniklých bezpečnostních incidentů, jejich

ohodnocení, popis možných dopadů, rizik a metodika postupu, jak je vyřešit

C.2. zvládání bezpečnostních incidentů:

C.2.1. hlášení bezpečnostních událostí, zejména:

C.2.1.1. ztráta služby, zařízení,

C.2.1.2. chybné fungování, přetížení systémů,

C.2.2., náprava bezpečnostního incidentu bude zahrnovat zejména:

C.2.2.1. analýzu a identifikaci příčiny incidentu,

C.2.2.2. plánování a implementaci opravných prostředků

C.2.2.3. hlášení kontaktním osobám

Kontaktní osoby	Společnost	E-mail	Telefon
l	3T Praha s.r.o.	<u>3t.cz</u>	
	ERÚ	<u>@eru.cz</u>	
	ERÚ	<u>s@eru.cz</u>	
	ERÚ	<u>@eru.cz</u>	
	ERÚ	<u>@eru.cz</u>	
	ERÚ	<u>@eru.cz</u>	

C.3. preventivní činnosti pro předcházení bezpečnostním incidentům, budou zahrnovat zejména:

C.3.1. automatické testování zranitelností, periodicky po vhodně zvolených intervalech,

C.3.2. generování výstrah a zdůraznění kritických zranitelností,

C.3.3. předávání zjištěných skutečností pověřenému pracovníkovi ERU

**D. Služby budou poskytovány v režimu 24 x 5 (24 hodin denně, 5 dní v týdnu) dle specifikace jednotlivých služeb**

**E. Způsob vykazování služeb:**

E.1. jedenkrát měsíčně souhrnná zpráva:

E.1.1. přehled o bezpečnostních incidentech a událostech za posledních 30 dní

E.1.1.1. objemy a druhy provozu za poslední měsíc,

E.1.1.2. statistika incidentů (podezřelých aktivit v síti ERU)

E.1.1.3. aktuální stav zabezpečení počítačů (verze antivirových vzorků apod.)

E.2. okamžitě při výskytu bezpečnostního incidentu (bezpečnostní incident vzniká, když např. na stupnici definované závažnosti od 1 do 10, má hodnotu 8 a vyšší):

E.2.1. čas zjištění zranitelnosti,

E.2.2. popis nalezené zranitelnosti,

E.2.3. provedená akce.

Cena měsíčního paušálu je 24.000,- Kč bez DPH.

S pozdravem

**Fakturu zašlete na výše uvedenou adresu s dobou splatnosti 21 dnů ode dne doručení.**