



G - Incident

Riešenie incidentov a útokov na IS

Máte vo vašej firme vypracovaný bezpečnostný plán pre prípad požiaru?

Vedia pracovníci, čo robiť pri úraze?

Ste teda pripravení naozaj na každý incident?

A viete, ako sa zachováte, keď odhalíte útok na váš informačný systém?

G - Incident

Riešenie incidentov a útokov na IS



Incident ohrozujúci bezpečnosť vášho informačného systému môže mať za následok únik alebo stratu cenných údajov, nepríjemnú zmenu obsahu vašej webovej stránky, ale aj odpočúvanie strategicky významných telefonátov alebo znefunkčnenie servera.

Ani najzabezpečenejšia sieťová infraštruktúra a konfigurácia informačného systému nedokáže ochrániť pred všetkými rizikami.

Podľa štúdie amerického inštitútu CSI z roku 2002 (1/2002 CSI/FBI Computer Crime and Security Survey):

- každoročne až 90% organizácií zistí narušenie bezpečnosti svojho informačného systému,
- v dôsledku čoho 80% organizácií utrpí reálne finančné straty,
- 38% organizácií zaznamenalo neautorizovaný prístup do webovských služieb,
- 40% organizácií bolo vystavených útokom ohrozujúcim dostupnosť služieb.

Vo firme, ktorá nie je pripravená na útok proti informačnému systému, dochádza po jeho odhalení spravidla k živelnému pokusu o riešenie. Zväčša prerastie do paniky a vzájomného obviňovania administrátorov. Vznikol bezpečnostný incident a nie je jasné, ako sa brániť. Všetci však vedia, že to treba urobiť rýchlo.

V takejto situácii je najlepšie zavolať GORDIAS.

Zo skúseností vieme, že väčšine strát je možné zabrániť rýchlym a adresným konaním – priamou akciou. Naši odborníci majú praktické skúsenosti s riešením rozličných bezpečnostných incidentov a postupujú podľa metodického plánu združenia CERT/CC (Computer Emergency Response Team).

Cieľom pri odstraňovaní následkov útoku na informačný systém je:

- minimalizácia strát (dáta, inštalované aplikácie, hardvér),
- minimalizácia výpadkov služieb informačného systému,
- zistenie podrobných informácií o útoku,
- zachovanie dobrého mena spoločnosti.

Pri útokoch väčších rozmerov odporúčame našim zákazníkom, aby zvažili aj možnosť osloviť orgány činné v trestnom konaní (aj tu je samozrejme možná spolupráca expertov spoločnosti GORDIAS).

Existujú však aj iné metódy riešenia útoku ako napríklad kontaktovanie správcu informačných technológií, ktoré použil útočník. Aj s takýmito procesmi má GORDIAS skúsenosti a sprostredkuje ich štandardným spôsobom.

Obráťte sa však na nás aj v opačnom prípade: ak vzniklo podozrenie, že útok ktorýmkoľvek smerom bol vykonaný pomocou vašich zariadení.

Významnú úlohu pri riešení bezpečnostných incidentov zohráva prevencia a pripravenosť.

Pripravenosť zákazníkov spoločnosti GORDIAS pozostáva:

- z vytvorenia procedúr a rámca pre riešenie bezpečnostných incidentov,
- z monitorovania podozrivých aktivít a detekcie incidentov,
- zo zaškolenia personálu na riešenie špecifických situácií,
- z overovania schopnosti personálu incidenty riešiť.

V prípade bezpečnostného incidentu volajte GORDIAS, s.r.o. / tel: 02/65315024

