SOCA
SOC powered by ANECT

BEZPEČNOSTNÍ HROZBY EXISTUJÍ, NEČEKEJTE NA ÚTOK NEBO NA NOVINÁŘE

V posledních dnech zintenzivnila diskuze o **kybernetické bezpečnosti**, na čemž má svůj podíl kauza okolo Ministerstva zahraničních věcí ČR.
Takzvaný **„hackerský útok"** na ministerstvo spočíval ve stahování informací z e-mailových schránek ministra Zaorálka i dalších úředníků. Jak dlouho útok trval, jak a proč ke kompromitaci došlo a co všechno mají útočníci k dispozici, to je momentálně předmětem šetření NBÚ a Národního centra kybernetické bezpečnosti.

Nejedná se o ojedinělý případ, většina společností v České republice není na podobné hrozby řádně připravena.

JAK JSTE NA TOM VY A VAŠE ORGANIZACE?

- **Jste si jisti, že nejste obětí podobného útoku?**
- **Jak je na tom s bezpečností vaše firma?**

S NÁMI NEMUSÍTE MÍT OBAVY

Provedeme rychlou revizi stavu vaší bezpečnosti a dáme vám jasnou zprávu o tom, kde jsou nedostatky a slabá místa.

- **Prověříme, kudy by se k vám útočníci mohli dostat**
- **Odhalíme, zda u vás už neoperují**
- **Zjistíme, zda vám neunikají citlivá data**

Věnujte pouze několik minut následujícím informacím, které můžeme nazvat malým kurzem kybersebeobrany. Díky včasnému odhalení existujících hrozeb a slabých míst můžete zabránit kritickému incidentu, který by mohl vážně poškodit nejen vaši IT infrastrukturu, ale i pověst a obchodní výsledky.

KDE ZAČÍT A JAK SE PODOBNÝCH INCIDENTŮ VYVAROVAT?

Účinná obrana začíná u správné konfigurace firewallů, aktualizace operačních systémů serverů a koncových stanic, aplikací a signatur v antivirovém software. Bohužel, je spíše pravidlem, že ani tento základní předpoklad obrany není splněn. Navíc platí, že proti moderním sofistikovaným útokům ani tyto základy nestačí. Naprosto nezbytné je si připustit nutnost neustálého sledování a revize stavu ICT bezpečnosti. Jejich kontrola vám umožní přijmout zavčas adekvátní opatření, čímž podstatně snížíte možná rizika a kritické dopady případného incidentu. Neméně důležité je také důkladné a kontinuální vzdělávání uživatelů, kteří často svou neznalostí hrozeb nevědomky útočníkům pomáhají.

NEJLEPŠÍ OBRANA JE DŮSLEDNOST!

Pokud nemáte čas, znalosti a nástroje pro naplnění těchto základních předpokladů účinné obrany proti kybernetickému zločinu, jste ohroženi třeba podobným typem útoku jako MZV.

Pokud byste chtěli svůj aktuální stav ICT bezpečnosti konzultovat, rádi vám pomůžeme.

Pro tyto účely Vám nabízíme služby **SOCA**, tedy dedikované SOC (Security Operations Center) centrum pro řízení bezpečnosti, za kterým stojí tým odborníků zajišťující **nepřetržitý monitoring** svěřené infrastruktury.

Provádíme analýzu událostí, řešíme incidenty, navrhujeme nápravná opatření a podílíme se na jejich implementaci.

<u>Značka kvality:</u>

SOCA je akreditovaným CSIRT týmem v rámci evropské CERT komunity (akreditace dle TF CSIRT Trusted Introducer)

UDĚLEJTE SI REVIZI STAVU ICT BEZPEČNOSTI

Hlídejte uživatele a jejich účty!

Mezi naprostý základ ICT bezpečnosti by měla patřit revize stavu účtů a přístupů do kritických systémů. Sledujte pečlivě životní cykly všech účtů, nepoužívané odstraňte, dodržujte zásady bezpečných hesel a důsledně spravujte uživatelská oprávnění.

Pozor na existující zranitelnosti a průniky!

Testování zranitelností a penetrační testování je nutnost, a to na všech úrovních přístupu (vnější, vnitřní, prostřednictvím aplikací). Současně je nezbytný dohled nad celkovým chováním uživatelů v interní síti, což pomáhá rychle odhalit nestandardní jevy. Včasná detekce kompromitovaných zařízení zabrání dlouhodobému útoku.

Testujte pravidelně!

Zavedením detekce a prevence malwaru pomocí sandboxing technologií eliminujete riziko, že se některý z uživatelů svou neopatrností zasadí o to, aby aktivoval či dokonce rozšířil nebezpečný malware.

Sledujte data!

V dnešní době jsou DLP (Data Loss Prevention) nástroje naprosto nepostradatelné. Sledujte důkladně, jak je s důležitými daty nakládáno. Jedině tak předejdete nechtěným únikům a zbytečným ztrátám.

CO TO KONKRÉTNĚ ZNAMENÁ?

PŘI ZJIŠTĚNÍ STAVU ZÁKLADNÍ KYBERNETICKÉ A INFORMAČNÍ BEZPEČNOSTI UDĚLEJTE:

Revizi aktuálního stavu účtů a přístupů do kritických systémů (včetně např. e-mailového systému), např. odstranit nepoužívané účty, zkontrolovat nastavení bezpečnostních funkcí, politiku hesel apod.
Kontrolu zranitelností a provedentí penetračních testů
  - Veřejně dostupných prvků z Internetu (perimetr)
  - Interních prvků (podle důležitosti pro organizaci, ale nevynechat ani ty méně důležité, i ty mohou být branou pro útočníka)
  - Aplikací
Revizi anomálního chování uživatelů a prvků v interní síti
Revizi efektivity stávajících bezpečnostních opatření na perimetru
Revizi architektury a strategie bezpečnostních opatření (technických i organizačních)

POKRAČUJTE ZJIŠTĚNÍM STAVU V OBLASTI POKROČILÝCH METOD OBRANY:

Revizí detekce a obrany proti pokročilému malwaru pomocí sandboxing nástrojů na jednotlivých komunikačních kanálech a na koncových stanicích
Detekcí kompromitovaných koncových stanic a serverů v interní síti
Revizí stavu zpracování a pohybu citlivých dat s využitím DLP se zaměřením především na komunikační kanály e-mail a web, na koncových stanicích a na datových úložištích (souborové servery, portály, cloud)

A JAK NAPRAVIT NEDOSTATKY?

Technická opatření

- Pravidelné nebo nejlépe průběžné testování zranitelností všech prvků ICT infrastruktury
- Nasazení řešení na obranu proti zranitelnostem nultého dne (např. detekce a prevence malware pomocí sandboxing technologií)
- Využití aplikačního firewallu pro obranu zranitelných webových aplikací
- Detekce anomálního chování uživatelů a prvků v síti
- Sledování pohybu a manipulace s citlivými daty
- Správa přístupu uživatelů, zejména privilegovaných, včetně silné autentizace
- Centrální sběr logů, jejich analýza a vyhodnocování bezpečnostních událostí

Organizační opatření

- Zajištění pravidelného bezpečnostního školení řadových uživatelů a administrátorů
- Nastavení postupů a procesů pro pravidelné vyhodnocování logů a nálezů z jednotlivých detekčních nástrojů
- Zavedení a pravidelné testování postupů okamžité reakce na kritické kybernetické bezpečnostní události a incidenty (tzv. mitigační scénáře)
- Zajištění kvalifikovaného vyhodnocování a reakce na bezpečnostní nálezy prostřednictvím:
  - Vnitřních odborných kapacit organizace (vybudování vlastního SOC týmu), nebo
  - Prostřednictvím SOC služeb externího dodavatele