

Kybernetická bezpečnost a chemické podniky Červenec 2021



Obrázek 1: Čistírna vody v Oldsmar na Floridě

Dne 5. února 2021 si zaměstnanec čistírny vody ve městě Oldsmar na Floridě všiml, že se na obrazovce řídicího systému divně pohybuje kurzor. Zpočátku ho to neznepokojilo, protože podnik používal software pro vzdálený přístup, který umožňoval zaměstnancům sdílet plochu obrazovky a řešit tak IT problémy. Jeho nadřízený se také často připojoval k operátorskému počítači, aby zkontroloval provozní systémy. O několik hodin později si operátor všiml pohybu kurzoru a klikání na ovládací prvky čistírny vody. Během několika sekund se narušitel pokoušel změnit v systému nastavenou hodnotu hydroxidu sodného ze 100 ppm na 11 100 ppm. Operátor toto narušení rychle zjistil a vrátil hodnotu hydroxidu sodného na normální úroveň. Naštěstí se to obešlo bez dopadu na kvalitu vody.

Nedávný útok vyděračským softwarem (ransomware) na společnost Colonial Pipeline zastavil na několik dní dodávky ropných produktů na východní pobřeží USA.

Systémy vaší společnosti jsou pravděpodobně připojeny k internetu a vyžadují ochranu před kybernetickými hrozbami. Společnosti využívají k ochraně před kybernetickými hrozbami mnoho strategií, například brány firewall, antivirový software a politiky ochrany před malwarem a počítačovými viry.

Na dálku teď pracuje více lidí. Zvýšilo se tím množství příležitostí pro kybernetické útoky.

Víte, že?

- Kybernetičtí zločinci používají sofistikované škodlivé programy (malware), aby využili řady zranitelností (chyb v zabezpečení) a dosáhli tak svých cílů.
- Počet vyděračských útoků roste s tím, jak je organizování zločinců používají jako nástroj pro vydělávání peněz.
- Podle nedávné studie dochází ke kybernetickému útoku každých 39 sekund (zdroj: <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>)
- Podvodné emailové útoky (phishing) od domnělých renomovaných společností mají za cíl přimět jednotlivce odhalit osobní údaje. Tyto útoky jsou primární metodou vstupu pro malware.
- Kybernetické hrozby se mohou dostat do systémů společnosti prostřednictvím e-mailů, příloh a z přenosných úložných zařízení jako jsou například flash disky nebo jiná přenosná úložná zařízení.
- Devadesát pět procent narušení kybernetické bezpečnosti je způsobeno lidskou chybou (zdroj: <https://www.cybintsolutions.com/employee-education-reduces-risk/>).

Co můžete udělat?

- Vždy si ověřte u IT požadavky na provedení aktualizace softwaru, a nainstalujte schválené aktualizace včas.
- Zajistěte, aby byly brány firewall a další síťový software aktuální a zapnuté.
- Pravidelně zálohujte svoje systémy a data.
- Pro všechny přístupy používejte silná hesla. Nesdílejte hesla ani uživatelské účty a hesla pravidelně měňte.
- Neukládejte hesla do webových prohlížečů.
- Neklikejte na odkazy nebo přílohy v e-mailech odesílaných od lidí, které neznáte.
- Nikdy neinstalujte neschválený software na žádný počítač společnosti. Ujistěte se, že přístupové klíče a další fyzická zabezpečovací zařízení jsou správně zabezpečena.
- Pokud používáte vzdálený přístup, postupujte podle požadavků společnosti. Při používání veřejných internetových stránek buďte obzvláště opatrní.
- Pokud se vám něco na vašem počítači zdá divné nebo jiné, požádejte o pomoc! Může to být hacker, který se snaží získat přístup.

Kybernetické útoky jsou skutečné. A Vy jste nepostradatelnou součástí obrany.