Process Safety Beacon
Wiadomości dla personelu produkcyjnego
www.aiche.org/ccps/process-safety-beacon

An AIChE Technology Alliance
CCPS Center for Chemical Process Safety
aiche.org/ccps

To wydanie sponsoruje
ioMosaic®
Minimizing risk. Maximizing potential.®
www.iomosaic.com

Cyberbezpieczeństwo a operacje z chemikaliami

Lipiec 2021

Zdjęcie 1. Oldmar, Floryda, instalacja uzdatniania wody

5 lutego 2021 pracownik stacji uzdatniania wody w Oldsmar na Florydzie zauważył, że kursor dziwnie porusza się na ekranie komputera sterującego. Początkowo nie było żadnych obaw; zakład używał bowiem oprogramowania do zdalnego dostępu, aby umożliwić pracownikom współdzielenie ekranów i rozwiązywanie problemów IT. Kierownik często łączył się z komputerem operatora, aby również monitorować systemy instalacji. Kilka godzin później operator zauważył, że kursor sam porusza się i klika kontrolki stacji uzdatniania wody.
W ciągu kilku sekund intruz próbował zmienić nastawę dla wodorotlenku sodu w systemie z wartości 100 ppm na 11100 ppm. Operator szybko zauważył nieuprawnione wtargnięcie i przywrócił normalny poziom nastawy wodorotlenku sodu. Na szczęście nie odnotowano żadnego wpływu na jakość wody.

Niedawno przeprowadzony atak ransomware na rurociąg Colonial pozbawił na kilka dni dostaw benzyny na wschodnie wybrzeże Stanów Zjednoczonych.

Systemy Twojej firmy są prawdopodobnie podłączone do Internetu i wymagają ochrony przed cyberzagrożeniami. Istnieje wiele strategii stosowanych przez firmy do eliminowania cyberzagrożeń, takich jak: firewall'e, oprogramowanie antywirusowe oraz polityki chroniące przed złośliwym oprogramowaniem i wirusami komputerowymi.

Więcej osób pracuje zdalnie; zwiększyło to możliwości cyberataków.

Czy wiedziałeś?

- Cyberprzestępcy wykorzystują zaawansowane złośliwe oprogramowanie, aby wykorzystać rozmaite luki w zabezpieczeniach i osiągnąć swoje cele.
- Liczba ataków typu ransomware rośnie, a zorganizowani przestępcy używają go jako narzędzia do zarabiania pieniędzy.
- Według ostatnich badań, co 39 sekund dochodzi do cyberataku (zobacz: https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds)
- Phishing to wysyłanie wiadomości e-mail, rzekomo od renomowanych firm, w celu nakłonienia osób do ujawnienia danych osobowych. Ataki te są podstawową metodą wejścia złośliwego oprogramowania.
- Cyberzagrożenia mogą przedostawać się do systemów firmy za pośrednictwem wiadomości e-mail, załączników i przenośnych urządzeń pamięci masowej, takich jak pendrive'y lub inne przenośne urządzenia pamięci masowej.
- 95% naruszeń bezpieczeństwa cybernetycznego jest spowodowanych błędami ludzkimi. (zobacz: https://www.cybintsolutions.com/employee-education-reduces-risk/)

Co możesz zrobić?

- Zawsze sprawdzaj żądania aktualizacji oprogramowania z działem IT przed wykonaniem tych czynności i instaluj zatwierdzone aktualizacje w odpowiednim czasie.
- Upewnij się, że firewall'e i inne oprogramowania sieciowe są aktualne i włączone.
- Upewnij się, że regularnie tworzysz kopie zapasowe systemów i danych.
- Używaj silnych haseł dla każdego dostępu. Nie udostępniaj haseł ani kont i regularnie zmieniaj hasła.
- Nie zapisuj haseł w przeglądarkach internetowych.
- Nie klikaj linków ani załączników w wiadomościach e-mail wysłanych od kogoś, kogo nie znasz.
- Nigdy nie instaluj niezatwierdzonego oprogramowania na żadnym firmowym komputerze; upewnij się, że klucze dostępu i inne fizyczne urządzenia zabezpieczające są odpowiednio zabezpieczone.
- Jeśli korzystasz ze zdalnego dostępu, postępuj zgodnie z wymaganiami firmy. Zachowaj szczególną czujność podczas korzystania z publicznych stron internetowych.
- Jeśli coś na twoim komputerze wydaje się dziwne lub inne, poproś o pomoc! Może to być haker próbujący uzyskać dostęp.

Cyberataki są realne. Ty jesteś istotną częścią obrony przed nimi.