Wielowymiarowa integracja sieci OT z sieciami IT niesie za sobą wiele korzyści. Usprawnienie procesów produkcyjnych i usługowych czy dokładniejsza analiza danych – to jedne z fundamentów rozwoju firm. Jednocześnie otwartość na komunikację ze światem zewnętrznym zwiększa podatność na cyberataki, także te skierowane na infrastrukturę przemysłową.

CYBER WYZWANIA 2023: Przedsiębiorcy wciąż nie są świadomi konieczności cyberochrony

Aleksander Kostuch, inżynier Stormshield fot. mat. prasowe Stormshield

> *„Sporo firm ma zaplecza informatyczne z gówna i patyków, przez zwykłą*

> *nieświadomość”* – tak specjaliści na jednym z forów dot. cyberbezpieczeństwa komentują niedawny (styczeń 2023), skuteczny atak ransomware na placówkę medyczną w Otwocku.*

Także eksperci Stormshield, europejskiego dostawcy rozwiązań bezpieczeństwa IT, zwracają uwagę, że wiele przedsiębiorstw wciąż nie jest świadomych konieczności ochrony własnych systemów oraz przypominają, że bezpieczeństwo nie jest dane raz na zawsze.

Cyberprzestępczość nie jest podatna na recesję

W opisywanym przypadku nieuprawniona osoba włamała się na serwer należący do placówki medycznej w Otwocku i zaszyfrowała zgromadzone na nim dane. Obejmują one imiona i nazwiska, numery PESEL, dane kontaktowe, dane medyczne pacjenta, w tym w szczególności dotyczące stanu zdrowia. Skutki ataku wydają być niezwykle poważne, podobnie jak konsekwencje dla firmy będącej dysponentem wrażliwych informacji.
Eksperci zwracają uwagę,
że przestępcy skupiają swoją uwagę nie tylko na usługodawcach, lecz także przedsiębiorstwach produkcyjnych, niezależnie od ich wielkości. Sprzyja im rozwój technologiczny sprawiający, że współczesna fabryka i jej systemy przemysłowe funkcjonują on-line.

> *– Rozwój technologiczny przyspiesza, a systemy OT w coraz większym stopniu wykorzystują Internet. Informacje dla systemów zarządzających procesami przekazywane są z wykorzystaniem wewnątrz-firmowych i zewnętrznych połączeń sieciowych, a za pośrednictwem Internetu w ramach połączeń szyfrowanych VPN odbywa się monitoring ich funkcjonowania,*

> *wsparcie techniczne oraz serwis. Pole do ataku jest spore, a warto mieć przy tym świadomość, że przestępcy rozwijają metody swojej działalności, aby uczynić ją maksymalnie skuteczną – komentuje Aleksander Kostuch, inżynier Stormshield.*

Z tego względu odpowiednie zabezpieczenie systemu OT pozostaje jednym z krytycznych elementów struktury bezpieczeństwa całej firmy. Skuteczny atak może mieć poważne implikacje, nawet wstrzymanie produkcji i będące jego konsekwencją straty finansowe i wizerunkowe.

> *– Przeświadczenie, że „mojej firmy to nie dotyczy" jest wciąż żywe, jednak o jego nieprawdziwości przekonujemy się dopiero wtedy, gdy sami doświadczymy ataku. Warto zawczasu sprawdzić, czy nie mamy zapóźnienia w obszarze bezpieczeństwa OT, które mogą okazać się kosztowne. Problem ten dotyczy dużych i średnich firm z różnych sektorów przemysłu. Zdecydowanie warto to potraktować w kategorii jednego z wyzwań na 2023 rok, bo cyberprzestępczość to jeden z niewielu sektorów gospodarki niepodatny na recesję – dodaje Aleksander Kostuch.*

Świadomość bycia na celowniku hakerów

Inną kluczową z perspektywy zagrożeń kwestią jest świadomość, że człowiek jest najczęstszym wektorem ataku. Dotyczy to każdego członka organizacji. Choć przestępcy celują w menadżerów, to również pracownik z ograniczonym dostępem do firmowych systemów może stać się koniem trojańskim, poprzez którego zostanie zaatakowana

organizacja. Rzeczywistość rynkowa jest taka, że wciąż spora grupa menadżerów polskich przedsiębiorstw nie posiada wiedzy z zakresu bezpieczeństwa IT, które z racji zajmowanych stanowisk posiadać powinni. Zdaniem eksperta wskazuje to na poważną lukę.

> *– Oceniam, że szansy, aby poznać fundamenty wiedzy, która pozwoliłaby im bardziej bezpiecznie funkcjonować w środowisku firmowym również z perspektywy bezpieczeństwa IT, mogła nie mieć nawet jedna trzecia osób na stanowiskach kluczowych. A przecież ci pracownicy znajdują się wśród głównych celów hakerów, za sprawą przydzielonych im wyższych uprawnień dostępowych do firmowych zasobów IT i OT. Jeśli połączymy to z informacjami takimi jak te z niedawnego raportu firmy Ivanti, to możemy zobrazować skalę wyzwania, z jakim musimy się mierzyć – komentuje Aleksander Kostuch, ekspert czołowego w Europie wytwórcy rozwiązań do bezpieczeństwa IT.*

W badaniu Ivanti 97 proc. ankietowanych specjalistów zadeklarowało, że organizacje na rzecz których działają są przygotowane do obrony przed cyberatakami, lecz jednocześnie aż 20 proc. z nich uznało, że i tak nie byliby w stanie im zapobiec.

Dlatego obok wprowadzania odpowiednich rozwiązań technicznych, takich jak nowoczesne firewalle np. NG UTM – SNS (Stormshield Network Security) czy Endpoint Security – SES (Stormshield Endpoint Security), niezmiennie istotne jest podnoszenie świadomości i kompetencji pracowników w zakresie cyberbezpieczeństwa. Zarówno osób technicznych, jak i pracowników nieposiadających specjalistycznej wiedzy. Warto nieustannie podnosić świadomość pracowników w zakresie zagrożeń, które się zmieniają.

> *– Dedykowane szkolenia dla personelu, dla szeregowych pracowników i kadry zarządzającej, aktualizujące wiedzę na temat bezpieczeństwa w cyberprzestrzeni są niezbędne najmniej raz w roku. Ta wiedza przyda się zarówno w pracy jak i w życiu prywatnym, gdzie również jesteśmy narażeni na ataki cybernetyczne – opiniuje Aleksander Kostuch.*

Gejmczendżer: Dyrektywa NIS 2

Niewątpliwie dobrą okazją, aby odnieść się do tego problemu będzie implementacja Dyrektywy NIS2. Konsekwencją modyfikacji unijnego prawodawstwa dotyczącego cyberbezpieczeństwa będą istotne zmiany w tym obszarze. W założeniach dyrektywy systemy zabezpieczeń powinny uwzględniać aktualny stan wiedzy i być proporcjonalne do ryzyka związanego z konkretną działalnością. Zdaniem eksperta Stormshield to oznacza również koncentrację na zagadnieniach związanych z obszarem OT, m.in. za sprawą ujęcia obowiązkami w zakresie zabezpieczeń branż, które do tej pory nie były traktowane jako sektory krytyczne.

> *– NIS2 wprowadza ideę, aby systemy zabezpieczeń były najnowsze ze względu na aktualny stan wiedzy i proporcjonalne do ryzyka związanego z konkretną działalnością. Rozszerzenie katalogu branż objętych prawodawstwem przekłada się na fakt, że obejmą one obszar OT. W szczególności należy wziąć pod uwagę dwa aspekty: detekcję incydentów teleinformatycznych oraz skuteczne reagowanie na nie. To znaczy, że z jednej strony nacisk kładziony jest na redukowanie negatywnych skutków wystąpienia incydentu lub zagrożenia bezpieczeństwa, przy czym NIS2*

> *kładzie również nacisk na uwzględnienie kryptografii i korzystanie z szyfrowania. Z drugiej strony należy podejmować działania prewencyjne – komentuje ekspert Stormshield.*

Jego zdaniem szybkie zaimplementowanie mechanizmów wspomagających ochronę własnej infrastruktury OT jest w obecnej sytuacji krokiem w dobrą stronę.

> *– Każdy przedsiębiorca we własnym interesie powinien przeanalizować te kwestie już teraz. Praktyczna implementacja rekomendowanych w ramach NIS2 rozwiązań może być czasochłonna. I choć przyjęcie nowego prawa wiązało się będzie z vacatio legis, to wobec skali wyzwania może się ono okazać niewystarczające. Oczywiście wiąże się to z inwestycjami, jednak zawsze lepiej przeciwdziałać zagrożeniom niż odczuwać skutki udanego ataku – podsumowuje Aleksander Kostuch.*

źródło informacji: Stormshield

*
https://sekurak.pl/ransomware-w-placowce-medycznej-w-otwocku-objete-incydentem-dane-pacjentow-z-5-lat-w-tym-dane-kontaktowe-wyniki-badan-dokumentacja-medyczna/#comments