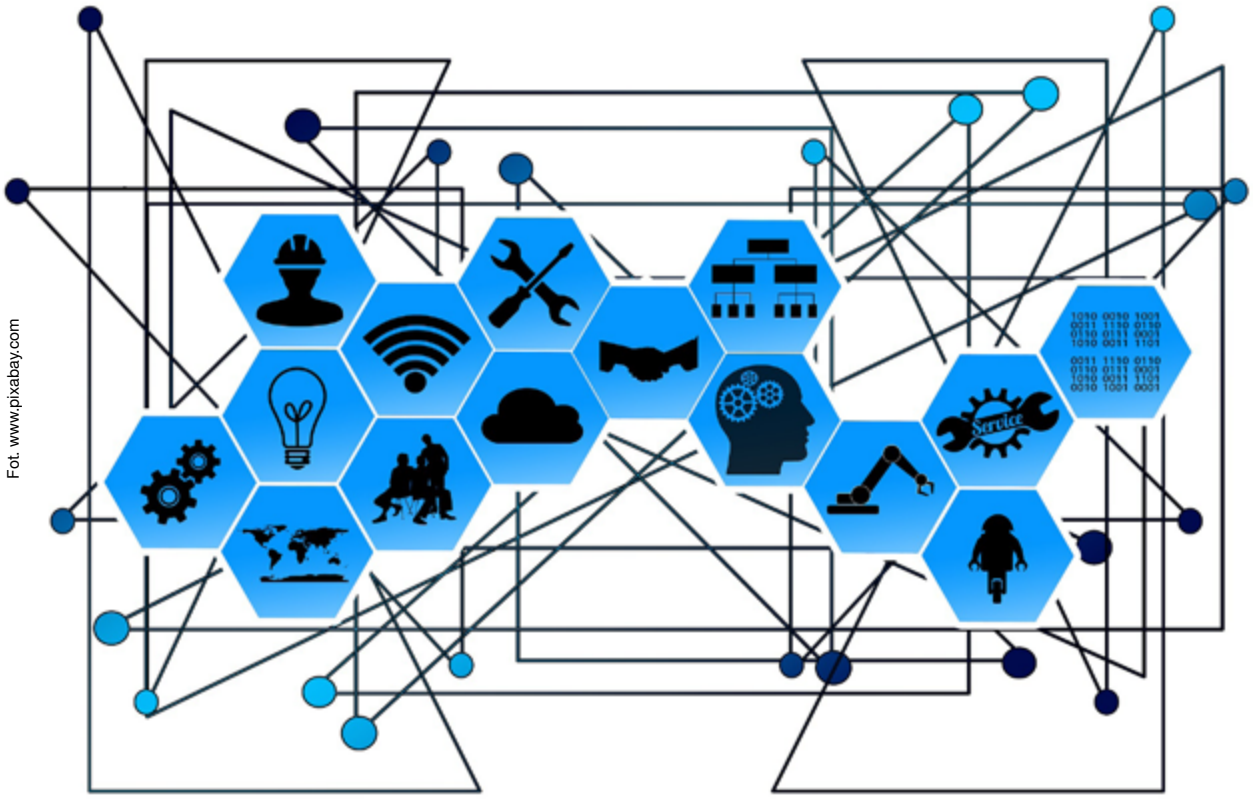
Adam Paturej,
Dyrektor Programu Cyberbezpieczeństwa, Fundacja Międzynarodowe Centrum Bezpieczeństwa Chemicznego

Nowa odsłona cyberbezpieczeństwa

- jak poradzić sobie w gąszczu norm, praktyk i nowych rozwiązań, aby zwiększyć niezawodność funkcjonowania firmy?



Fot. www.pixabay.com

O cyberbezpieczeństwie najczęściej słyszymy w mediach w przypadku ataków na konta bankowe oraz sieci społecznościowe. Kojarzymy ją z przestrzenią komputerów, sieci. Rzadziej jednak myślimy, jak ona przekłada się na realne działanie firm. W firmach przemysłowych wirtualne ataki mogą przybrać bardzo realną i widzialną formę w przypadku, kiedy procesy technologiczne wymkną się spod kontroli (atak na rafinerię Saudi Aramco, albo lokalny wodociąg Oldsmar na Florydzie). Czy jedyną formą zabezpieczeń jest instalacja kolejnego systemu oraz nowej technologii? Czy potrzebny jest inny zestaw działań?

Obserwując rynek od dłuższego czasu uwidacznia się, że wiele firm, albo oddala od siebie problem cyberbezpieczeństwa (najczęściej twierdząc, że są zbyt mali, aby ich to dotyczyło), albo inwestuje duże pieniądze w systemy, które nie są w stanie pokryć całości zagrożeń - szczególnie w warstwie produkcyjnej, bądź systemów sterowania.

Cyberbezpieczeństwo jest trudnym zagadnieniem dla firm z uwagi na częsty brak widzialnych metryk. Próbuje się je wskazać poprzez potencjalne ataki i ilość odbitych połączeń, ale ma to niewielki związek z prawdziwymi zagrożeniami. Z tego powodu - z punktu widzenia zarządu - wydatki na cyberbezpieczeństwo są kosztem, który choć konieczny, ciężko uzasadnić inwestycyjnie. Z drugiej strony, kiedy pojawia się nowe rozwiązanie technologiczne, które obiecuje rozwiązać problem cyberbezpieczeństwa, często firmy po instalacji mają problem z dalszym utrzymaniem tych systemów poprzez brak zasobów i przestają one spełniać swoją funkcję.

Firmy produkcyjne z założenia pracują w porządku i pewnej przewidywalności. Świat sztywnych połączeń elektronicznych odszedł dawno w niepamięć, a skomplikowanie systemów, powszechne protokoły spowodowały, że zapanowanie nad wszystkimi funkcjami sterowników przemysłowych stało się wręcz niewykonalne. Kiedyś sterownik PLC dysponował prostym rejestrem wejść i wyjść z ograniczoną pamięcią. Obecnie jest to de facto komputer z szybkim procesorem i serwerem dostępnym na żądanie w warstwie TCP/IP. Dla menedżerów produkcji, którzy rekomendują zakup sprzętu zarządowi coraz trudniej odnaleźć się w gąszczu nowych funkcji i wymagań. Paradoksalnie wiele z tych funkcji zwiększa zagrożenia z punktu widzenia cyberbezpieczeństwa!

Jak zatem się bronić?

Pierwszym i najważniejszym etapem obrony jest uznanie przez decydentów firmy, że problem cyberbezpieczeństwa jest jednym z wielu aspektów leżący w ich kompetencjach (a nie wąsko w dziale IT). Dla zarządu, funkcjonowanie firmy to multum zagrożeń, począwszy od zagrożeń finansowych, braku kadr, po zmiany prawne, wymogi samorządowe/państwowe, bądź środowiskowe. I tak samo jak zarząd dysponuje narzędziami do radzenia sobie z każdym z powyższych zagadnień, tak są metody dostępne dla każdego (a nie tylko dla informatyków), które mogą pomóc wesprzeć firmę w programie cyberbezpieczeństwa. Wyzwaniem jest to, że zaczynając pracę nad takim programem szybko okazuje się, że okala on każdy dział w firmie, stąd tak ważne jest sprawne kierowanie procesem przez zarząd. Dalsze brnięcie w nowoczesne systemy nie jest wcale odpowiedzią na istniejące już problemy technologiczne. Wskażmy to na przykładach.

> Pierwszym i najważniejszym etapem obrony jest uznanie przez decydentów firmy, że problem cyberbezpieczeństwa jest jednym z wielu aspektów leżący w ich kompetencjach - a nie wąsko w dziale IT

Przykłady

W branży znany jest przypadek, w którym całość dobrze zabezpieczonego procesu technologicznego został zniweczony przez usterkę w systemie chłodzenia (traktowany jako poboczny). Odpowiedzmy sobie na pytanie: czym jest to co produkujemy i jakie zasoby są w tym procesie kluczowe? Bez których zasobów nie uda nam się dostarczyć produktu, a które systemy możemy zastąpić i jakim kosztem? Zbudowanie sieci powiązań między sprzętem informatycznym, a innymi niezbędnymi procesami powinno nam uwidocznić systemy, które powinniśmy chronić w pierwszej kolejności. Taka sieć powiązań może wydawać się na pierwszy rzut oka oczywista, ale szybko uporządkuje to wiedzę na temat zależności w funkcjonowaniu firmy oraz da odpowiedź w analizie, które zasoby są kluczowe przy budżetowaniu inwestycji, bądź modernizacji instalacji.

Fot. Markus Spiske on Unsplash

W obecnym świecie wiele powiązań nie jest już tak oczywista jak ta powyżej (tu uwidacznia się skomplikowanie technologii). Jeśli myślimy, że wymiana informacji ze sterownika PLC następuję tylko i wyłącznie z komputera sterującego (albo lokalnego HMI, albo dalszego z sieci SCADA), to często okazuje się, że jesteśmy w błędzie. Szczególnie w dobie tzw. inteligentnych sensorów. Idąc dalej tą ścieżką szybko dojdziemy do wniosku, że najbardziej wrażliwą na ataki jest na przykład stacja inżynierska, która wgrywa program wykonawczy do głównych sterowników przemysłowych. W jaki sposób chronimy ten kluczowy zasób? Czy dostęp do niego ma technik, który przyjeżdża raz na jakiś czas do naszej firmy (czy są odpowiednie rejestry), czy na przykład każda osoba, która dysponuje pamięcią USB?

Kolejnym aspektem jest, jak radzimy sobie z incydentem, którego i tak nie unikniemy. Jak szybko jesteśmy w stanie przywrócić pierwotną produkcję w przypadku zaburzenia? Czy jesteśmy w stanie proces technologiczny uruchomić ręcznie? Jak zabezpieczamy kluczowe aktywa takie jak programy sterujące procesem technologicznym? Jak zarządzamy zmianą oraz opisem aktualizacji tych programów wykonawczych? Czy polegamy na zewnętrznej firmie, czy może mamy zasoby wewnętrznie, aby poradzić sobie z problemem szybciej?

Budowa programu cyberbezpieczeństwa

Analiza powyższa, która skutkuje przygotowaniem mapy powiązań, kluczowych zasobów i systemów jest pierwszym krokiem do budowy programu cyberbezpieczeństwa (który tutaj wychodzi poza ramy ochrony informacji, czy ochrony komputerów). Odpowiadając na pytanie postawione na początku, program cyberbezpieczeństwa nie wymaga wcale zaawansowanej technologii, czy wiedzy stricte informatycznej. Do tej pory większość zaleceń z norm cyberbezpieczeństwa jest prewencyjna i nie wskazuje, które konkretnie komputery trzeba zabezpieczać (mówi się, że wszystkie, co jest ani technicznie, ani organizacyjnie niemożliwe). Przykłady: Zamknij nieużywane połączenia na firewallu, zadbaj o to, by wyłączyć dostęp zwalnianym pracownikom, itd. Są to rzeczy niekwestionowanie ważne, ale z punktu widzenia analizy ryzyka dla zarządu suche stosowanie norm bez analizy kluczowych zasobów i potencjalnych konsekwencji będzie skazane na porażkę. W programie cyberbezpieczeństwa nie chodzi o budowaniu metryk o ilości zaktualizowanych łat bezpieczeństwa w systemie operacyjnym, ale o przygotowanie się na odpowiednią reakcję w sytuacji krytycznej.

> Wyposażając w odpowiednie narzędzia zarząd, inżynierów oraz techników można odpowiednio zbudować program niezawodności dla firmy

Powyżej ukazany został wstęp do całościowej metodyki, którą szerzej omówimy podczas nadchodzącej **VII Konferencji „Niezawodność i Cyberbezpieczeństwo Infrastruktury Krytycznej i Przemysłowej IT/OT”** w Warszawie w dniach 7-8 września 2022. Podczas niej wskażemy dalsze przykłady, że dyskusja o cyberbezpieczeństwie nie może być jedynie analizą techniczną zabezpieczeń komputera, czy sieci. Wyposażając w odpowiednie narzędzia zarząd, inżynierów oraz techników można odpowiednio zbudować program cyberbezpieczeństwa, który zwiększa niezawodność funkcjonowania firmy. A taki program daje już konkretne korzyści inwestycyjne, gdyż zmniejsza on przypadkowość w produkcji, a nie tylko punktowo zabezpiecza wybrane komputery. □