Nie można wyciągnąć wtyczki

W wielu przedsiębiorstwach znajdują się podsieci z urządzeniami szczególnie wrażliwymi na atak, takimi jak systemy SCADA. Powszechną praktyką jest separacja sieci, ale nie zawsze jest to możliwe.

MARCIN MARCINIAK

Przez wiele lat nie było potrzeby wprowadzania specjalnych zabezpieczeń do środowisk automatyki przemysłowej, gdyż były to sieci całkowicie odseparowane. Gdy sieci IP stały się standardem, rozpoczął się proces stopniowej migracji do połączeń za pomocą IP. Kolejnym etapem stało się wprowadzanie interfejsów webowych, które są łatwe w obsłudze i zapewniają kontrolę z dowolnego miejsca, także z innej sieci. Łatwość łączenia sieci IP oraz korzyści biznesowe sprawiają, że coraz częściej oba segmenty są ze sobą integrowane. Niekiedy odbywa się to z rażącym naruszeniem podstawowych zasad bezpieczeństwa. Powstanie przeznaczonych do tego celu wyszukiwarek, takich jak Shodan, sprawia, że napastnik bez problemów znajduje podatne urządzenia i przy minimalnym wysiłku przeprowadza atak.

Czy można „wyciągnąć wtyczkę"?

Chociaż naturalnym rozwiązaniem ochrony może być powrót do separacji (w tym osobne urządzenia i brak przenoszenia plików z zewnątrz), model ten nie będzie spełniać potrzeb biznesu. Zamknięcie dostępu do zasobów sieci technologicznych sprawia, że znajdujących się tam informacji nie będzie można analizować, a zatem nie da się uzyskać wartości, która się w nich znajduje. Niemożliwe staje się antycypowanie problemów, poszukiwanie anomalii wskazujących na naturalne zużycie podzespołów lub nadchodzące problemy techniczne. Tymczasem analiza danych i konsultacje z partnerem technologicznym mogą przyczynić się do zmniejszenia kosztów eksploatacji urządzeń, a także pomóc przy unikaniu nieplanowanych przestojów.

Diagnostyka jako źródło wiedzy w zarządzaniu majątkiem

Podczas 17. Sympozjum Pro Novum omawiane były zagadnienia związane z diagnostyką jako źródłem wiedzy w zarządzaniu majątkiem. Jednym z ważnych wniosków była możliwość określenia symptomów zbliżającej się awarii. Prowadzone badania połączone z analizą ryzyka umożliwiają optymalną eksploatację urządzeń. Działania te można usprawnić, określając prawdopodobieństwo awarii, koszty przestojów, a także optymalnie zaplanować okna serwisowe. Analiza danych pochodzących z eksploatacji pod kątem planowania napraw jest stosowana w wielu branżach (m.in. w transporcie lotniczym, w dużych centrach przetwarzania danych, w przemyśle), gdzie przynosi istotne korzyści biznesowe. Wymaga to jednak połączenia z siecią technologiczną.

Jak zabezpieczyć sieć technologiczną

Sieć urządzeń automatyki przemysłowej zarządzających obsługą procesów technologicznych jest dość statyczna.

Wszelkie zmiany wprowadzane są tam względnie wolno, model połączeń oraz stosowane protokoły są znane od początku wdrożenia i pozostają niezmienne przez lata. W takiej sieci obcego ruchu w ogóle być nie powinno i można wprowadzić zasadę białych list, a także zdefiniować działanie punktów styku między siecią technologiczną a wydzieloną podsiecią IT. W tych punktach styku będzie odbywać się wymiana informacji między systemami zarządzania przedsiębiorstwem a serwerami w sieci technologicznej. Wprowadzanie zasady ograniczonego zaufania do pozostałych sieci umożliwia minimalizację ryzyka związanego z zagrożeniem cybernetycznym przychodzącym z tych obszarów, w których kontrola IT jest ograniczona.

Podobny model w praktyce zastosowała Energa-Operator, wdrażając zabezpieczenia sieci technologicznej TAN w ramach projektu BBS-TAN (bezpieczeństwo brzegu sieci technologicznej).

Najważniejsze elementy wprowadzonej ochrony sieci TAN obejmują:

- zasadę zerowego zaufania do ruchu spoza podsieci (usunięcie skrośnych połączeń na brzegu sieci TAN);
- klasyfikację ruchu na podstawie protokołów, a nie portów i adresów;
- uwierzytelnienie użytkowników (a nie tylko adresów IP);
- inspekcję ruchu razem z detekcją intruzów oraz prewencją sieciową;
- narzędzia wykrywające obecność złośliwego oprogramowania;
- deszyfrowanie ruchu SSL na punkcie styku, analizę pod kątem anomalii;
- wdrożenie dwuskładnikowego uwierzytelnienia, wymaganego do zalogowania się użytkowników w obrębie sieci TAN;
- brak dostępu do internetu (włącznie z brakiem routingu);
- terminowanie połączeń na brzegu z użyciem chronionych i specjalnych aplikacji;
- prowadzenie regularnych audytów zabezpieczeń;
- wdrożenie systemów korelacji zdarzeń, połączonego z systemem zarządzania konfiguracją oraz kopiami bezpieczeństwa;
- wdrożenie procedur i rozwiązań umożliwiających szybkie przywrócenie kompletnej konfiguracji do stanu ostatniej dobrej konfiguracji.

Okna podatności

Podobnie jak w klasycznych systemach IT w przypadku automatyki przemysłowej również występuje zjawisko nazywane oknem podatności. Polega ono na tym, że po wykryciu luki (usługi, urządzenia, oprogramowania, całego rozwiązania) następuje atak za pomocą eksploita wykorzystującego daną podatność. Infrastruktura pozostaje jednak nadal podatna do czasu, aż producent rozwiązania opracuje aktualizację usuwającą daną podatność i łata zostanie wprowadzona w danej sieci. W przypadku rozwiązań automatyki przemysłowej proces usuwania podatności trwa znacznie dłużej niż w zwykłych środowiskach IT.