OpenBIZ Sp. z o.o.

Jak zapewnić rzetelny pomiar ryzyka IT/OT?

Systemy wytwarzania oraz przesyłu energii ewoluują. Powstanie paradygmatu Smart Grid, wprowadzenie odnawialnych źródeł energii oraz nowych sposobów jej gromadzenia wymaga, aby sieci i systemy stawały się coraz bardziej elastyczne w zakresie swojego funkcjonowania. Powoduje to, że automatyczne sterowanie siecią staje się czynnikiem kluczowym w całym cyklu dostawy - poczynając od wytworzenia, poprzez transmisję, a na odczycie liczników konsumenckich (IED) kończąc.

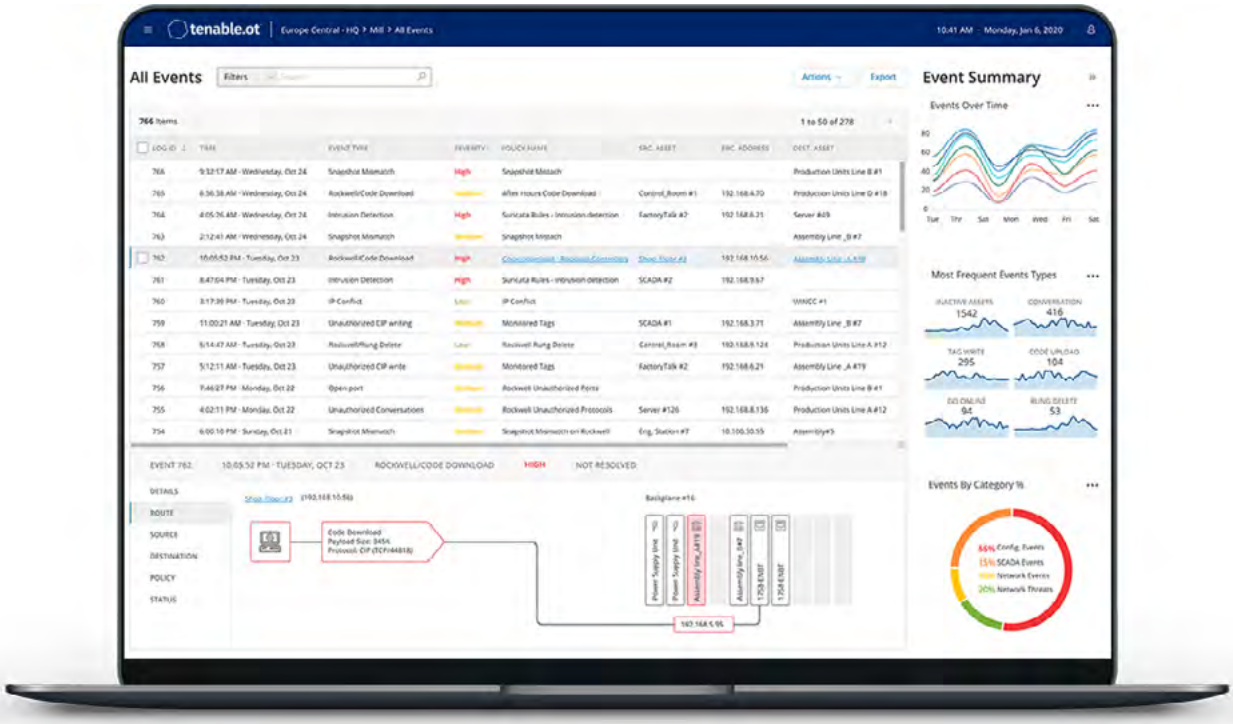
Ale automatyzacja i cyfryzacja procesu transferu i zarządzania energią niesie za sobą poważne zagrożenia. W maju 2021 na skutek ataku na Colonial Pipeline, operatora rurociągów w USA, dostępu do benzyny i ropy pozbawionych zostało 45% użytkowników na wschodnim wybrzeżu USA, a cena za galon paliwa skoczyła z 3 do 7 USD. Okup jaki operator zapłacił atakującym wyniósł wedle doniesień prasowych pięć mln dolarów.

Nie był to wypadek odosobniony, bowiem w przeciągu kilku ostatnich lat ofiarami ataków padły takie giganty jak: Aramco, Norsk Hydro, Elexon, Light S.A. of Brazil, LTI Power Systems, INA Group of Croatia, czy Tajwańska państwowa firma energetyczna CPC Corp. Przed atakiem nie ustrzegł się nawet European Network of Transmission System Operators for Electricity (ENTSO-E), który 9 marca 2021 ogłosił, że padł ofiarą skutecznego ataku ransomware.

Czy zatem unikać automatyzacji i cyfryzacji w imię zachowania odpowiedniego poziomu bezpieczeństwa? Oczywiście nie. Nie da się bowiem odejść od modernizacji i unowocześnienia, natomiast należy to robić po inżyniersku, czyli: świadomie, rzetelnie, skutecznie, mierzalnie oraz, nader wszystko, bezpiecznie. Należy zatem uwzględniać zarówno wymogi norm branżowych (IEC-61850, IEC-60870-5-104, ISO-27001, ISO-22301), jak aktów normatywnych: zaleceń NIS EU oraz polskiej Ustawy o Krajowym Systemie Cyberbezpieczeństwa.

> „bezpieczeństwo to nie jest stan, bezpieczeństwo to proces fluktuujący w funkcji czasu”

Systemy zautomatyzowane mają tendencję do szybkiej ewolucji i dużej zmienności, dlatego rzeczą niezmiernie ważną jest trafne i rzetelne ich monitorowanie, również od strony bezpieczeństwa IT/OT. Zagrożenie bowiem stanowią nie tylko błędy w konfiguracji, ale również ujawniane z czasem błędy w oprogramowaniu sterowników i urządzeń kontrolnych oraz aktywność intruzów, którzy coraz częściej atakują nie świetnie chronione firewallami i bacznie nadzorowane punkty styku sieci firmowych z Internetem, ale skupiają się na uzyskiwaniu bezpośredniego dostępu do sieci w stacjach pomiarowych lub skrzynkach atmosferycznych. Kolejnym istotnym czynnikiem ryzyka są firmy współpracujące z operatorami. Coraz częściej bowiem spotykamy się ostatnio z sytuacjami, w których firmy współ-



pracujące instalują bez wiedzy i zgody operatora urządzenia dostępowe oparte o modemy LTE, w celu uzyskania zdalnego dostępu do zainstalowanych systemów, a tym samym skrócenia czasu swojej reakcji na zgłoszenia. Takie „pluskwy" są zwykle bardzo słabo zabezpieczone i nie są nadzorowane przez piony bezpieczeństwa operatorów, zapewniając tym samym atakującemu łatwe uzyskanie dostępu do sieci. Konsekwencje są oczywiste.

Na co zatem zwrócić uwagę? Jak skutecznie monitorować systemy IT/OT i szacować pojawiające się w nich ryzyko? Wyjść należy od fundamentalnej tezy: „bezpieczeństwo to nie jest stan, bezpieczeństwo to proces fluktuujący w funkcji czasu". Jeżeli organizacja opiera swoje bezpieczeństwo (czy też: miary ryzyka) o dokonywane raz do roku testy penetracyjne i audyty, to należy przyjąć, że nie jest świadoma swojego ryzyka i nim nie zarządza.

Jakie są zatem główne czynniki zagrożeń? Można podzielić je na dwie grupy: wynikające z podejścia oraz stricte techniczne.

Czynniki ryzyka wynikające z podejścia:

- bezrefleksyjne (bez należytej analizy zagrożeń) przyjęcie paradygmatów Przemysłu 4.0 oraz Smart Grid - skutkuje to wprowadzeniem do konserwatywnej i nastawionej na niezawodność infrastruktury OT niefrasobliwości typowej dla świata IT. W świecie IT restart serwera nie jest niczym niezwykłym, w systemach OT restart sterownika ma zwykle bardzo poważne konsekwencje,
- likwidacja (bądź zmniejszenie znaczenia) dotychczas stosowanych paradygmatów bezpieczeństwa (vide: dioda danych w modelu Purdue) na rzecz wzrostu funkcjonalności dzięki ściślejszej integracji OT z IT,
- mała ilość wykwalifikowanych specjalistów potrafiących bezpiecznie łączyć IT z OT, określanych w branży jako „ITmatic" - czyli połączenie automatyka z informatykiem.

Techniczne czynniki ryzyka:

- łatwa penetracja systemów OT z sieci IT, wynikająca z ryzyka podejścia opisanego powyżej, a tym samym łatwa propagacja zagrożeń. Konsekwencjami tego stanu rzeczy są m. in. udane ataki na Colonial Pipeline, czy Norsk Hydro,
- wykrywanie nowych podatności w urządzeniach OT - żadne oprogramowanie nie jest pozbawione wad, tyczy się to również oprogramowania systemowego (firmware) w sterownikach OT,
- nieautoryzowane zmiany w nastawach sterowników - powodowane uszkodzeniem pamięci, błędem ludzkim lub działaniem intruza,
- obce, nieautoryzowane, urządzenia w sieci, zarówno wstawiane przez podwykonawców, jak i przez intruzów,
- błędy w konfiguracji sieci (tzw. bypass), skutkujące możliwością realizacji połączeń pomiędzy segmentami sieci (systemami), które powinny być odseparowane,

- brak ciągłego, powtarzalnego i mierzalnego procesu monitorowania i oceny ryzyk towarzyszących systemom sterującym.

Jak zatem trafnie i rzetelnie mierzyć ryzyko związane z systemami OT oraz z punktem/punktami styku z IT? Podstawowymi wymogami są:

- Pomiar powinien być ciągły (a nie raz na jakiś czas), najlepiej w czasie rzeczywistym lub zbliżonym do rzeczywistego.
- Zgodnie z zasadą, że „bezpieczeństwo to nie stan, ale proces" do mierzenia i analizy ryzyka powinien być wykorzystywany cykl Deminga, gwarantujący skuteczność i powtarzalność działań nadzorczych.
- Systemy IT powinny być skanowane aktywnie (bądź z wykorzystaniem agentów), natomiast systemy OT powinny być nadzorowane wyłącznie pasywnie, jako że skan aktywny urządzenia OT w większości wypadków spowoduje jego dysfunkcję.
- Wyjątkiem od powyższej zasady jest stosowanie technologii **Active Query**, polegającej na aktywnym odpytywaniu urządzeń OT z wykorzystaniem zapytań nieinwazyjnych, czyli stosowanych przez systemy SCADA/DCS/MCS do natywnego monitorowania automatyki.
- Snifowanie pasywne sieci OT powinno również pozwalać na wykrywanie anomalii (obcy ruch, niestandardowy ruch, bypassy pomiędzy sieciami), ale również na detekcję aktywności intruzów i wrogich działań wewnątrz sieci.
- System monitoringu powinien prowadzić pełen, aktualizowany automatycznie, wykaz zasobów w sieci, tak aby móc w czasie rzeczywistym wykrywać pojawienie się nowych (potencjalnie nieautoryzowanych, lub błędnie podłączonych) zasobów lub zniknięcie istniejących.
- System musi potrafić generować raporty i zestawienia obrazujące poziom ryzyka, zarówno na poziomie zarządczym, jak i technicznym.
- System musi mieć możliwość zautomatyzowanego raportowania w czasie rzeczywistym wykrytych ryzyk i ataków do systemów SOC.
- System powinien udostępniać API (interfejs programistyczny), w celu umożliwienia integracji z systemami zarządzania oraz nadzoru bezpieczeństwa.

Na rynku oferowanych jest w chwili obecnej kilka systemów realizujących pomiar ryzyka OT. Obsługują go jednak cząstkowo. Zwykle skupiają się wyłącznie na analizie ruchu pasywnego i jego anomalii, co powoduje następujące problemy: jeżeli sondy analizujące ruch nie są umieszczone na każdej podstacji i w każdej skrzynce atmosferycznej (ergo: zbierają ruch wyłącznie w Centrali i na węzłach głównych), to nie są w stanie wychwycić:

- podłączenia obcego urządzenia, ze szczególnym uwzględnieniem takich, które realizują nieautoryzowane połączenia do sieci publicznej (np. przez LTE),
- nieautoryzowanej modyfikacji firmware urządzeń OT lub ich nastaw (jak często bada się konfigurację SIS?),
- snifowania połączeń w danej lokalizacji w celu wykrycia anomalii oraz ataków,
- nieautoryzowanych zmian nastaw urządzeń OT (jak często badana jest konfiguracja operacyjna **wszystkich** urządzeń?).

Jedynym obecnie systemem, który jest w stanie uwzględnić wszystkie zagrożenia jest tenable.ot firmy Tenable Inc. Poza analizą pasywną ruchu sieciowego generowanego w danej lokalizacji/sieci potrafi on również odpytać urządzenia OT o wersje firmware, specyfikację nastaw oraz o zmiany w konfiguracji (wraz z przechowywaniem ich historii). Nie ma zatem potrzeby umieszczania w każdym backplane karty sensora **tenable.ot**. Wszystkie testy mogą odbywać się z poziomu systemu centralnego. Co niezmierne ważne - **tenable.ot** dokonuje badania systemów OT z wykorzystaniem opatentowanej technologii **Active Query** gwarantującej, że zapytania wysyłane do urządzenie będą zgodne ze standardami opracowanymi przez producenta OT, zatem, że nie spowodują dysfunkcji badanych systemów.

Tenable.ot zapewnia również detekcję ataków, anomalii sieciowych oraz wykrywa obce (nieautoryzowane) urządzenia i bypassy sieciowe, zatem nieuprawnione połączenia pomiędzy sieciami. System transmituje w czasie rzeczywistym informacje do systemów SIEM, pozwalając na ich analizę przez SOC, ale również dokonuje wymiany danych z tenable.sc (Security Center), systemem służącym do kompleksowej analizy ryzyka obszaru IT.

Prawidłowe wdrożenie systemu tenable.ot zapewnia nie tylko pełną widoczność wszystkich czynników ryzyka, ale stanowi również spełnienie wymogów nadchodzącej modyfikacji unijnego rozporządzania NIS, a tym samym wymogów noweli Ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC). OpenBIZ Sp. z o.o., polski Platynowy Partner firmy Tenable Inc. posiada wiedzę i doświadczenie pozwalające na efektywne wdrożenie systemu tenable.ot oraz jego integrację z funkcjonującymi w organizacji regulacjami. □

OpenBIZ

tenable ASSURE PLATINUM PARTNER

tenable.ot SPECIALIST

www.openbiz.pl

Platynowy Partner Tenable Inc. w Polsce. Autoryzowany dostawca systemów i usług bezpieczeństwa OT/IT oraz compliance