Patryk Gęborys, lider Obszaru Bezpieczeństwa Systemów Przemysłowych,
Kamil Kowalczuk, ekspert bezpieczeństwa, Zespół Cyber Security PwC Polska

Pewnego razu na Ukrainie...

Było mroźne grudniowe popołudnie. W jednej z dyspozytorni firmy Kievoblenergo obsługującej sieć dystrybucji w regionie kijowskim na zachodniej Ukrainie operatorzy szykowali się do zdania swojej zmiany i pójścia do domu. Nagle jeden z nich zauważył niecodzienne zachowanie się swojej konsoli systemu sterującego siecią elektroenergetyczną. Kursor myszy zaczął sam poruszać się po ekranie w stronę opcji sterowania rozłącznikami. Zdziwiony pracownik obserwował jak na ekranie zaczęły otwierać się kolejne okienka systemu i kolejne rejony energetyczne były odcinane od głównych linii dystrybucyjnych. Próby odzyskania kontroli nad konsolami w całym centrum nie przynosiły rezultatu. Chwilę później ekran systemu zgasł...

Systemy OT - co to jest i dlaczego są ważne?

Opisany scenariusz nie jest wzięty z książki fantastyczno-naukowej, ani nawet z thrillera politycznego. 23 grudnia 2015 r. ponad 230 000 odbiorców energii elektrycznej w regionie podkarpackim utraciło dostęp do energii elektrycznej na skutek nie „tradycyjnej" awarii, czy klęski żywiołowej, ale w rezultacie cyberataku na infrastrukturę krytyczną. Tym razem zasilanie udało się przywrócić w ciągu maksymalnie 6 godz., przy czym wiele stacji transformatorowych działa w trybie ręcznego sterowania.

Nie trzeba nikogo przekonywać, że systemy automatyki przemysłowej - systemy SCADA, DCS, czy bardziej ogólnie - systemy *Operational Technology* (OT) - są sercem dzisiejszej energetyki. Jeszcze kilkanaście lat temu nikt ich nie nazywał istotnym elementem infrastruktury krytycznej. System tego rodzaju był postrzegany jako ważny element infrastruktury, którego funkcjonowanie było kluczowe do zapewnienia ochrony i bezpieczeństwa energetycznego kraju. Jednak zawsze można było przejść na sterowanie ręczne. Wróćmy do dnia obecnego, czy bylibyśmy w stanie przejść, w pełnym zakresie na sterowanie ręczne? Byłoby to bardzo trudne, wręcz niemożliwe. Systemy OT zoptymalizowały sposób pracy przedsiębiorstw w sektorze energetycznym. Próba powrotu do sterowania ręcznego wymagałaby przeorganizowania pracy, co nie odbyłoby się bez ryzyka utraty ciągłości dostaw. Wyobraźmy sobie, że wyłączamy system sterowania i nadzoru w elektrowni czy sieci dystrybucyjnej, albo w elektrociepłowni czy tłoczni. Wyobraźmy sobie, że wyłączamy dostawy do krajowej sieci przesyłowej, tym samym wpływamy na całe społeczeństwo i gospodarkę kraju. Zarówno w obszarze wytwarzania, jak i dystrybucji - bez nich nikt nie wyobraża sobie, nie tylko sprawnie, ale w ogóle działającej sieci czy instalacji elektroenergetycznej. Jeśli coś zadziała inaczej niż powinno lub nie zadziała wcale, efekty mogą nieść straty finansowe, środowiskowe, a także ludzkie.

Aktualny krajobraz zagrożeń dla systemów OT

Architektura i sposób pracy systemów OT nie odbiega w dużym stopniu od innych systemów IT. Podstawowa różnica to ranga systemu i kontekst. System OT jest nie tylko kluczowy dla funkcjonowania firmy z sektora energetycznego, ale również ingeruje w prawidłowe i stabilne funkcjonowanie państwa.

System OT vs. ICT

Pracując w biurze wielokrotnie korzystamy z edytora tekstu. Piszemy

jakąś notatkę czy pismo, a następnie kilkoma sprawnymi ruchami myszki klikamy przycisk „Drukuj". Po chwili mamy wydrukowany dokument na kartce papieru. Tego typu działania w świecie ICT *(ang. Information and Communication Technologies)* są czymś naturalnym. Niewiele jest zdarzeń utrudniających naszą pracę. W systemie OT kliknięcie może spowodować zmianę parametrów urządzenia, takiego jak sprężarka czy kocioł w bloku energetycznym. Decyzje podejmowane przy pomocy myszki i klawiatury mają wpływ na pracę całej elektrowni - mają wpływ na bezpieczeństwo osób i mienia.

Uruchomionego raz systemu OT nie można ot tak wyłączyć. Jego wyłączenie, w przeciwieństwie do typowego systemu IT, jest niezwykle trudne i ogromnie kosztowne.

Bezpieczeństwo

Wyróżnia się trzy elementarne funkcje bezpieczeństwa: poufność, dostępność i integralność.

Poufność - funkcja bezpieczeństwa wskazująca obszar, w którym dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom. W odniesieniu do naszej organizacji jest to zapewnienie odpowiedniego poziomu dostępu do informacji, niezbędnego z punktu widzenie wykonywanych obowiązków. Przykładem jest dostęp do danych przechowywanych w systemie Dyspozytorskim oraz zapewnienie go wyłącznie osobom, które ze względu na charakter swojej pracy, muszą je przetwarzać. Innym ważnym aspektem, ze względu na swoją działalność statutową, jest ograniczenie dostępu do procedur stanowiskowych systemów OT, opracowań technicznych.

Integralność - funkcja bezpieczeństwa odnosząca się do danych (informacji). Dane nie uległy zniekształceniu (nie zostały zmienione, dodane lub usunięte) w nieautoryzowany sposób. Przykładem jest proces wymiany danych pomiędzy dwoma odrębnymi systemami lub systemem, a operatorem (HMI). W procesie ich uzyskiwania nie nastąpiła niekontrolowana zmiana, np. poprzez błąd systemu lub działanie szkodliwego oprogramowania ingerującego w system. Integralność jest niezwykle istotna dla systemów transakcyjnych, sterowania oraz obrazowania. W badanym obszarze integralność danych ma również znaczenie w zakresie przekazania informacji niskopoziomowo, np. z i do PLC (urządzenie przeznaczone do sterowania pracą maszyny lub urządzeń) do Systemu Dyspozytorskiego.

IT	OT
Brak powiązań wprost między systemami a celami biznesowymi;	Jasne powiązanie celu biznesowego (proces technologiczny);
Wiele aplikacji, dostarczających różne funkcje na komputerze, czy serwerze;	Komputer, czy serwer realizujący jedną funkcje;
Wiele zmian w cyklu życia systemów;	Mała ilość zmian systemu w jego cyklu życia;
Wiele wymagań prawnych (Dane osobowe, KNF);	Brak zdefiniowanych, jednoznacznych wymagań prawnych;
Relatywnie prosta implementacja poprawek i wycofania zmian;	Trudny proces testowania poprawek, czy często duża trudność wycofania poprawek;
Błędy ludzkie mało wpływające na bezpieczeństwo życia ludzkiego;	Błędy ludzkie, które mają wpływ na bezpieczeństwo życia ludzi;
Powszechny dostęp do sieci Internet	Ograniczony lub usunięty dostęp do sieci Internet

Rys. 1. Główne różnice między systemami IT, a OT

Dostępność - jest to cecha informacji mówiąca o tym, że w dookreślonym czasie i miejscu użytkownik może ją uzyskać. Podstawowym przykładem jest uzyskanie informacji z systemu OT przez użytkownika.

Dla większości systemów IT prezentujących informacje przyjmuje się, że największą wagę ma poufność. Zgodnie z tą zasadą najwięcej czasu i energii poświęca się poufności informacji. Systemy OT prezentują głównie dane chwilowe, które za kilka minut nie mają większego znaczenia i nie stanowią tak dużej wartości. Dla systemów sterowania i nadzoru najistotniejszy funkcje to dostępność i integralność danych - aby osoby nadzorujące ruch czy sterujące pracą bloków energetycznych mogły podjąć decyzje w sposób, w pełni świadomy i szybko w zależności od potrzeb.

Skupmy się na chwilę, na integralności. Zafałszowane dane o pracy urządzeń mogą spowodować ich uszkodzenie. Przykładem jest tutaj podawanie w Iranie błędnych parametrów pracy wirówek do wzbogacania uranu - robak Stuxnet w 2010 r. Kolejnym przykładem jest zaburzenie procesu wytwórczego stali w 2014 r., w jednej z niemieckich hut. Zaburzenie procesu wytapiania stali spowodowało zamknięcie wielkiego pieca, powodując ogromne uszkodzenia i straty dla firmy.

Wiele incydentów bezpieczeństwa spowodowanych przez złośliwe oprogramowanie jest diagnozowana jako awaria, a nie typowy atak na instalacje.

Dlaczego dostępność jest tak ważna? Ponieważ nagłe wyłączenie bloku energetycznego czy elektrociepłowni, albo tłoczni gazu może być w zasadzie niemożliwe. Przykładem takiego ataku było zablokowanie dostępu do systemu dyspozytorskiego jednej z elektrowni atomowych w USA, w 2003 r. Robak Slammer (nie był on dedykowany dla systemów OT) spowodował utratę kontroli nad systemem nadzoru. Na szczęście obyło się bez katastrofy nuklearnej.

Wielu naszych pracowników pracuje w terenie i brak należytego nadzoru nad siecią dystrybucyjną, np. w trakcie prac elektroniebezpiecznych, może spowodować wypadek. Brak dostępu do systemu OT lub zafałszowane in-

formacje mogą się przekładać na kwestie życia lub śmierci, nie wspominając o uszkodzeniu instalacji technologicznych.

Wielokrotnie systemy OT nie były projektowane z myślą o bezpieczeństwie danych. Wiele wykorzystywanych protokołów transmisji, np. w procesie sterowania, nie były projektowane z założeniem, że mają być bezpieczne, ale funkcjonalne. Nikt nie przypuszczał, że rozwój technologii, potrzeby biznesowe mogą doprowadzić do tego, że systemy OT w równym, jak i większym stopniu będą wymagały większej uwagi w kontekście bezpieczeństwa. Rozdzielenie fizyczne obu światów jest coraz trudniejsze. Wielokrotnie to potrzeby rynku obniżenie kosztów i zwiększenie efektywności oraz zintegrowanie rozproszonych źródeł energii wymusza zmianę optyki na bezpieczeństwo Systemów OT - przykład to Smart Grid (inteligentne sieci elektroenergetyczne).

Liczba ataków i podatności

Biorąc pod uwagę znaczenie systemów OT w USA, w ramach Departamentu Bezpieczeństwa Wewnętrznego *(Department of Homeland Security)*, powołano jednostkę odpowiedzialną za reagowanie na zagrożenia cybernetyczne w obszarze systemów nadzoru przemysłowego, która działa na zasadach znanych już zespołów CERT w obszarze systemów teleinformatycznych. Prócz reagowania na incydenty i wsparcia merytorycznego, ICS-CERT publikuje statystyki incydentów w systemach przemysłowych. Na rysunku 2. można zauważyć trend wzrostowy w odniesieniu do ilości zarejestrowanych incydentów i podatności. Pamiętać należy, że są to dane ilościowe dotyczące tylko zgłoszonych zdarzeń. Nadal znacząca część incydentów, albo nie jest zgłaszana, albo nie jest wykrywana.

Większość systemów nadzoru przemysłowego działa w oparciu o standardowe systemy informatyczne, wykorzystując systemy operacyjne, np. MS Windows, bazy danych takie jak: MS SQL, czy też sieci lub macierze dyskowe. Nie da się mówić o bezpieczeństwie systemów nadzoru przemysłowego, jeżeli nie zapewnimy bezpieczeństwa w każdej warstwie architektury rozwiązań. Biorąc pod uwagę fakt, iż średni czas życia systemów nadzoru przemysłowego przekracza

Rys. 2. Trend wzrostowy w odniesieniu do ilości zarejestrowanych incydentów i podatności

15 lat i najczęściej dostawca nie umożliwia wdrażania poprawek bezpieczeństwa, wyobrażenie skali problemu może dać rysunek 3., pokazujący trend w ilości odkrytych podatności systemów teleinformatycznych na przestrzeni ostatnich 18 lat.

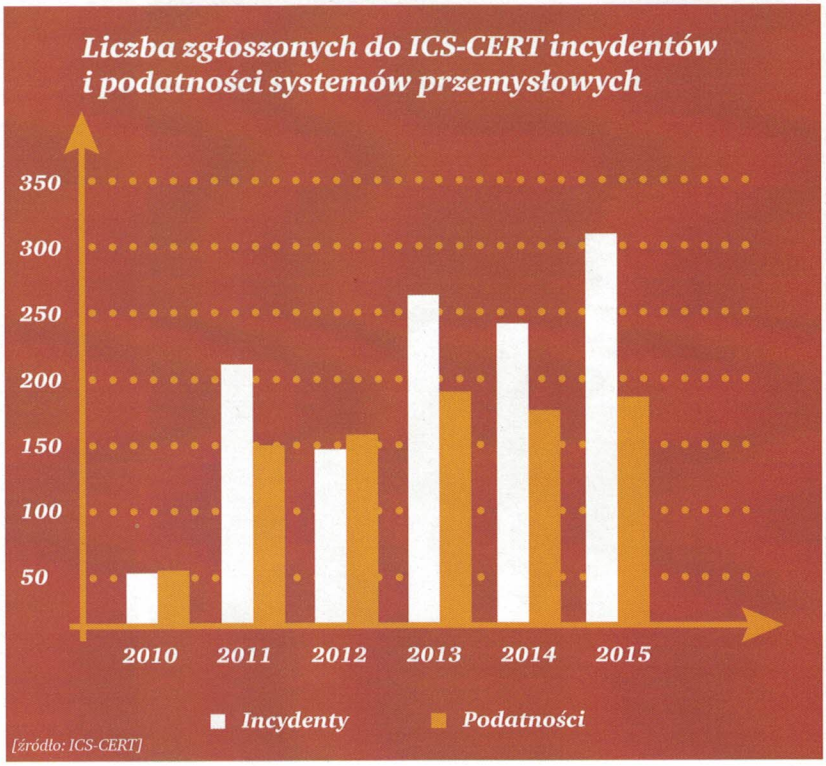
Z kim się mierzymy?

Wzrost liczby znalezionych luk i standaryzacja oprogramowania przekłada się wprost na zainteresowanie różnych grup interesów. W cyberprzestrzeni, do tej pory, obserwowaliśmy głównie działalności zorganizowanych grup przestępczych oraz nieuczciwych konkurentów, którzy są nastawieni na osiągnięcie korzyści finansowych lub przejęcie know-how. Według ekspertów, zyski z działalności w sieci już dawno przekroczyły te osiągane z „tradycyjnych" gałęzi przestępczości, takich jak narkotyki czy prostytucja. Równocześnie taka działalność jeszcze do niedawna była zagrożona dużo mniejszymi sankcjami prawnymi.

Jednak nie cyberprzestępcy są głównymi graczami w rozgrywce o kontrolę nad systemami OT. Jeśli zgodzimy się, że elektrownie, sieci elektroenergetyczne, wodociągi, inne zakłady użyteczności publicznej są sercem współczesnego państwa, to głównymi zainteresowanymi w jego zdobyciu mogą być terroryści oraz organizacje wspierane przez rządy państw. Cyberprzestrzeń od dawna jest uznana przez wojskowych strategów jako jedno z pól bitwy. Uzyskanie kontroli nad jak największą częścią infrastruktury krytycznej przeciwnika może wprowadzić chaos na jego tyłach uniemożliwiając lub utrudniając obronę. Wojna hybrydowa, wykorzystująca elementy walki tradycyjnej oraz elektronicznej, a także rozmycie granicy między działaniami wojennymi i sabotażem na stałe zagościła w arsenale współczesnych armii.

Co mogło się wydarzyć na Ukrainie - szczegóły

A więc co się wydarzyło owego feralnego grudniowego popołudnia na Ukrainie? Analiza doniesień wskazuje, że zostały zaatakowane równocześnie 3 zakłady energetyczne. Atak był przygotowywane wiele miesięcy i wykorzystywał wiele technik, co wskazuje na duże zaawansowanie i determinację atakujących. Najpierw należało uzyskać dostęp do wewnętrznej sieci teleinformatycznej. W tym celu wykorzystano ataki typu *spearphishing*, czyli wiadomości mailowe ze specjalnie spreparowanymi załącznikami w postaci plików pakietu Ms Office zawierającymi złośliwe oprogramowanie. Załączniki wyglądały całkowicie niewinnie, zachęcając odbiorców do ich otworzenia, co powodowało uruchomienie wirusów i otwarcie drzwi hake-



Rys. 3. Trend w ilości odkrytych podatności systemów teleinformatycznych na przestrzeni ostatnich 18 lat

rom do wewnętrznych sieci. Następnie spędzili oni wiele miesięcy na poznaniu wewnętrznych struktur i znalezieniu sposobu na przeniknięcie do chronionych systemów sterujących siecią elektroenergetyczną. Oprócz zastosowania oprogramowania umożliwiającego przejęcie kontroli nad stacjami operatorskimi, atakujący zadbali o utrudnienie przywrócenia właściwego działania i wprowadzenie dodatkowego chaosu. Po ataku wyłączyli systemy UPS podtrzymujące prace systemu dyspozytorskiego, a same stacje dyspozytorskie zostały zniszczone przy pomocy oprogramowania Killdisk, uniemożliwiając ich restart. Dodatkowo urządzenia komunikacyjne pozwalające na dostęp poprzez sieć teleinformatyczną do kontrolerów sterujących rozłącznikami zostały uszkodzone, zmuszając do przejścia na ręczne sterowanie i wysłanie do każdej stacji ekip pogotowia energetycznego. Dlatego w niektórych rejonach przerwa w dostawie trwała, aż 6 godz.

Dodajmy, że zaatakowane firmy miały wiele mechanizmów utrudniających, w założeniu, przeniknięcie do wrażliwych sieci, takich jak segmentacja, zapory ogniowe, itp. Jednak wiele z nich było także wdrożonych nieprawidłowo, np. zdalny dostęp bez dodatkowego uwierzytelnienia. Fakt ten potwierdza skuteczny atak przeprowadzony miesiąc później, wykorzystując zbliżony scenariusz na lotnisko, na Ukrainie.

Nowe obszary w elektroenergetyce - OZE, AMI, smart grids - nowy impact

Bez wątpienia atak na ukraińską sieć elektroenergetyczną pokazał z całą mocą, że zdeterminowany i wyposażony w duże środki przeciwnik jest w stanie zdestabilizować, krytyczne dla funkcjonowania współczesnego społeczeństwa, funkcje. Biorąc pod uwagę obecne kierunki rozwoju energetyki - odnawialne źródła energii, inteligentne opomiarowanie klientów *(ang. Advanced Metering Infrastracture)* i niezbędne do ich działania inteligentne sieci elektroenergetyczne (tzw. smart grids), należy się spodziewać, że zaintereso-

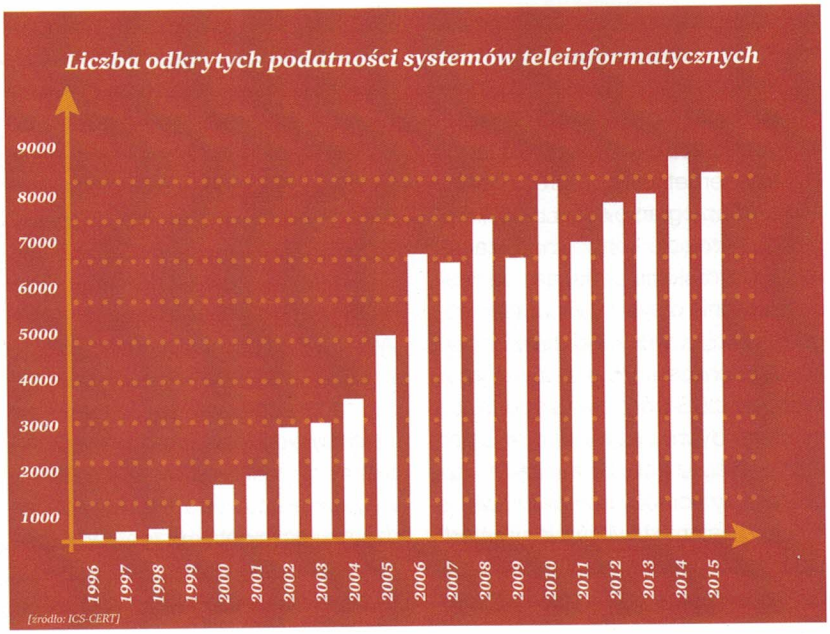
wanie tym obszarem będzie rosło. Należy się spodziewać, że wszystkie wymienione wcześniej grupy atakujących znajdą niszę dla siebie - od prób nadużyć w opłatach za energię elektryczną przez zorganizowanie grupy przestępcze po próby doprowadzania do spektakularnych awarii, którymi mogą być zainteresowani cyberterroryści, czy przejęcia kontroli nad infrastrukturą krytyczną przez wrogie państwo.

Wnioski z przypadku ukraińskiego oraz innych incydentów związanych z atakami na systemy sterującymi procesami przemysłowymi wskazują, że tego typu przypadki będą coraz częściej. W szczególności, że w zbliżony sposób zaatakowano port lotniczy na Ukrainie zaledwie miesiąc po opisywanym zdarzeniu.

Kluczowymi czynnikami, które pozwolą zminimalizować ich wpływ są według nas:

- Rozpoznanie swojego środowiska - tylko dobre rozpoznanie aktywów i ich priorytetyzacja pozwala na skierowanie środków w najistotniejsze, z punktu widzenia biznesu, zabezpieczenia. Tu pomoże audyt bezpieczeństwa środowiska IT i OT, który zidentyfikuje co działa dobrze, a jakie obszary wymagają szczególnej uwagi.
- Zabezpieczenie i monitorowanie - działające procesy są tak samo istotne, jak techniczne środki ochrony. Każde zabezpieczenie powinno być monitorowane i weryfikowane. Na Ukrainie nie było mechanizmów, które pozwalałyby na wykrycie trwającej wiele miesięcy infiltracji... Głównym działaniem w tym obszarze, powinno być wdrożenie adekwatnych systemów i procedur ochrony oraz monitorowania bezpieczeństwa, poprzedzone analizą wspomnianą w punkcie wyżej - co chronić i w jakim zakresie.
- Zaufanie i kontrola - partnerzy biznesowi stają się najsłabszym aktywem, w miarę jak podnosi się poziom bezpieczeństwa wewnętrznego. Wymagajmy od nich tak samo, jak od siebie. W tym zakresie z pomocą może przyjść weryfikacja stanu bezpieczeństwa partnerów biznesowych poprzez audyt zewnętrzny lub siłami własnymi. Pamiętajmy o zagwarantowaniu sobie takiej możliwości w umowach.
- Znajomość otoczenia i swoich wrogów - większość kampanii wymierzonych w konkretne organizacje ma swój prolog na forach internetowych. Rozpoznanie atakujących i ich motywów ułatwi przygotowanie linii obrony. Threat Intelligence jest obszarem wartym zainteresowania i wykorzystania - bieżące śledzenie i pozyskiwanie informacji nt. zagrożeń i śledzenie działań, które mogą skutkować atakiem.
- Przygotowanie - pomimo wszystkich zabiegów, incydent bezpieczeństwa jest kwestią czasu. Przygotowanie i przetestowanie zawczasu mechanizmów reakcji na incydenty jest jedynym sposobem na uniknięcie chaosu, gdy incydent wreszcie się wydarzy - a wydarzy się na pewno...

□



Rys. 4. Liczba odkrytych podatności systemów teleinformatycznych