

Opis luk w zabezpieczeniach systemu SCADA

WEWNĄTRZ

- > Typowe mylne wyobrażenia na temat zabezpieczeń systemu SCADA
- > Typowe luki w zabezpieczeniach sieci SCADA
- > Taktyka wzmacniania zabezpieczeń systemu SCADA

Spis treści

Streszczenie.	3
Typowe mylne wyobrażenia na temat zabezpieczeń systemu SCADA.	4
Typowe luki w zabezpieczeniach sieci SCADA.	5
Taktyka wzmacniania zabezpieczeń systemu SCADA.	7

> Streszczenie

W październiku roku 1999 pewien haker publicznie ogłosił zamiar opublikowania raportu opisującego, w jaki sposób można się włamać do sieci informatycznych elektrowni i wyłączyć sieć energetyczną 30 firm użyteczności publicznej¹. To zdarzenie, które zbiegło się w czasie z ostrzeżeniami jednej z rządowych agencji, głoszącej że „jedna osoba, dysponująca komputerem, modemem i linią telefoniczną w dowolnym miejscu świata, prawdopodobnie jest w stanie... spowodować przerwę w dostawie prądu w całym regionie”², poskutkowało wzmożonym zainteresowaniem branży energetycznej tematyką bezpieczeństwa sieci.

Powyższe zdarzenia wywołały zagorzałą dyskusję na temat poziomu bezpieczeństwa podstawowych dla działania firmy systemów stosowanych w firmach użyteczności publicznej (powszechnie zwanych systemami SCADA – z angielskiego „supervisory control and data acquisition systems”, czyli systemy sterowania nadzorczego i gromadzenia danych). Niniejszy raport, w którym wykorzystano wiarygodne informacje zebrane w ramach analiz stanu zabezpieczeń w wielu największych północnoamerykańskich firmach użyteczności publicznej, rzuca światło na sprawę rzeczywistej podatności na atak sieci informatycznych należących do firm użyteczności publicznej. Artykuł objaśnia również rodzaje luk w zabezpieczeniach powszechnie spotykane w firmach użyteczności publicznej, a także opis strategii zaradczych, jakie firmy użyteczności publicznej powinny przyjąć w celu zmniejszenia zagrożenia.

1. „The Next Y2K?” *Utilities IT*, luty 2000 r.

2. John Tritak, dyrektor biura Critical Infrastructure Assurance Office (CIAO), sprostżenia cytowane w artykule „The Next Y2K?” *Utilities IT*, luty 2000 r.

> Typowe mylne wyobrażenia na temat zabezpieczeń systemu SCADA

Źródłem problemu zabezpieczeń systemu SCADA są trzy główne mylne wyobrażenia, których zazwyczaj trzyma się kierownictwo firm użyteczności publicznej. Z doświadczeń ekspertów firmy Symantec w dziedzinie bezpieczeństwa sieci wynika, że główną przeszkodę we wdrożeniu najlepszych możliwych strategii zabezpieczeń informatycznych stanowią wymienione poniżej mylne wyobrażenia.

MYLNE WYOBRAŻENIE NR 1 – „SYSTEM SCADA ZNAJDUJE SIĘ W ODDZIELONEJ FIZYCZNIE, ODREBNEJ SIECI”

Większość systemów SCADA tworzono przed innymi sieciami korporacyjnymi, a nierzadko niezależnie od nich. Wskutek tego menedżerowie ds. IT zazwyczaj przyjmują założenie, że do systemów tych nie można uzyskać dostępu przez sieci korporacyjne ani ze zdalnych punktów dostępu. Niestety, przeważnie przekonanie to mija się z rzeczywistością.

W rzeczywistości między sieciami SCADA i korporacyjnymi systemami informatycznymi często istnieje fizyczne połączenie, powstałe w wyniku wprowadzenia dwu ważnych zmian w metodach zarządzania informacjami. Pierwsza z nich została wywołana zapotrzebowaniem na zdalny dostęp do informacji: wiele firm użyteczności publicznej utworzyło łącza do systemu SCADA, aby umożliwić inżynierom systemu SCADA jego nadzorowanie i sterowanie nim z punktów dostępu znajdujących się w sieci korporacyjnej. Po drugie, w wielu firmach użyteczności publicznej utworzono łącza między sieciami korporacyjnymi a sieciami SCADA, aby umożliwić wyższemu kierownictwu natychmiastowy dostęp do najważniejszych danych związanych ze stanem systemów eksploatacyjnych. Nierzadko łącza są zakładane bez pełnej wiedzy na temat zagrożeń związanych z taką operacją. W strategiach zabezpieczeń podstawowej infrastruktury informatycznej, stosowanych w firmach użyteczności publicznej, rzadko brany jest pod uwagę fakt, że uzyskanie dostępu do sieci korporacyjnej otwiera możliwość nieupoważnionego dostępu i przejęcia kontroli nad systemem SCADA.

MYLNE WYOBRAŻENIE NR 2 – „ŁĄCZA MIĘDZY SYSTEMAMI SCADA A INNYMI SIECIAMI KORPORACYJNYMI SĄ CHRONIONE SILNYMI ZABEZPIECZENIAMI DOSTĘPU”

Wiele połączeń wzajemnych między sieciami korporacyjnymi a systemami SCADA wymaga zintegrowania systemów, w których stosowane są różne standardy komunikacyjne. W wyniku często powstaje infrastruktura zaprojektowana do skutecznego przenoszenia danych między dwoma nietypowymi systemami. Złożoność integracji całkowicie odmiennych systemów sprawia, że konstruktorzy sieci często nie dają sobie rady z wdrożeniem odpowiednich zabezpieczeń lub wręcz nie zadają sobie z tym trudu. Środki kontroli dostępu, mające chronić systemy SCADA przed nieupoważnionym dostępem poprzez sieci korporacyjne, są w związku z tym minimalne. W dużym stopniu zaniedbanie to można przypisać faktowi, że osoby zarządzające siecią z łatwością przeocząją najważniejsze punkty dostępu łączące owe sieci. Chociaż bezwzględnie zalecane jest używanie wewnętrznych zapór ogniowych i systemów wykrywania włamań (IDS) w połączeniu z regułami wymuszającymi stosowanie silnych haseł, tylko w nielicznych firmach użyteczności publicznej wszystkie punkty dostępu do sieci SCADA są chronione w zalecany sposób.

MYLNE WYOBRAŻENIE NR 3 – „SYSTEMY SCADA WYMAGAJĄ SPECJALISTYCZNEJ WIEDZY, DZIĘKI CZEMU
WŁAMYWACZOM SIECIOWYM TRUDNO JEST UZYSKAĆ DO NICH DOSTĘP I PRZEJĄĆ KONTROLĘ”

Powyższe mylne wyobrażenie opiera się na założeniu, że nikt, kto atakuje dany system SCADA, nie ma możliwości uzyskania informacji na temat jego projektu i realizacji. Założenia te są nietrafne już choćby ze względu na zmiany charakteru luk zabezpieczeń w systemach firm użyteczności publicznej, będące skutkiem połączenia środowisk sieciowych. Firmy użyteczności publicznej, stanowiące główny element jednej z najważniejszych infrastruktur każdego państwa, są więcej niż prawdopodobnym celem skoordynowanych ataków „cyberterrorystów”. Są oni znakomicie zorganizowani, w odróżnieniu od działających w pojedynkę „hakerów”. Cyberterrorysty mają silną motywację, solidne fundusze, a nierzadko również wiedzę, dostępną rzekomo tylko osobom wtajemniczonym. Co więcej, dobrze wyposażona grupa napastników, której celem jest wyłączenie dostaw zapewnianych przez firmy użyteczności publicznej, nie cofnie się przed zdobyciem szczegółowych informacji o systemach SCADA i możliwych lukach w ich zabezpieczeniach przy użyciu wszelkich dostępnych środków.

Ryzyko dodatkowo powiększa rosnąca dostępność informacji na temat sposobu działania systemów SCADA. W ramach zwiększania konkurencyjności produktów opublikowano kilka standardów wzajemnego łączenia systemów SCADA i jednostek terminali zdalnych (RTU), takich jak standardy dotyczące komunikacji między ośrodkami sterowania, przyjmowania alarmów, przekazywania sterowania i sondowania obiektów danych. Ponadto dostawcy systemów SCADA publikują dokumentację projektową i obsługową produktów, a także sprzedają zestawy narzędzi umożliwiające tworzenie oprogramowania zgodnego z różnymi standardami stosowanymi w środowiskach SCADA.

Na domiar złego starania firm użyteczności publicznej, mające na celu jak najlepsze wykorzystanie informacji gromadzonych w systemie SCADA we wszystkich działach firmy, doprowadziły do opracowania „otwartego” standardu systemów SCADA. Zabezpieczenia systemu SCADA mają w związku z tym często tylko taką samą skuteczność, jak zabezpieczenia sieci korporacyjnej firmy użyteczności publicznej. Uzyskanie dostępu do terminali zdalnych w sieci spoza wydzielonych łączy szeregowych może być trudne, ale już włamanie do panelu sterowania menedżera systemu SCADA przez sieć korporacyjną stanowi umiarkowane wyzwanie. Wówczas wystarczy obserwować operacje na ekranie, aby szybko się nauczyć właściwych poleceń. Ataki na bardzo skomplikowane systemy stają się znacznie łatwiejsze, jeśli włamywacz najpierw zdoła przejąć kontrolę nad stacjami roboczymi operatorów systemu SCADA.

> **Typowe luki w zabezpieczeniach sieci SCADA**

Jak już wspomniano wyżej, sieci korporacyjne i systemy SCADA są często połączone, a to znaczy, że zabezpieczenia systemu SCADA są tylko tak skuteczne, jak zabezpieczenia sieci korporacyjnej. Wskutek działań wymuszających zmniejszenie poziomu kontroli na rzecz szybkiego wdrożenia funkcji otwartego dostępu podatność sieci korporacyjnych na ataki gwałtownie wzrasta. W dalszej części artykułu opisano kilka typowych luk w zabezpieczeniach systemów SCADA i sieci korporacyjnych, które zmniejszają względne bezpieczeństwo systemów SCADA.

Publiczna dostępność informacji

Zbyt często i zbyt wiele informacji na temat sieci korporacyjnych firm użyteczności publicznej można z łatwością uzyskać z ogólnodostępnych źródeł. Informacje te mogą posłużyć do przeprowadzenia bardziej precyzyjnego ataku na sieć.

Poniżej podano przykłady tego typu luk w zabezpieczeniach:

- Witryny sieci WWW często zawierają przydatne włamywaczom sieciowym informacje o strukturze organizacyjnej firmy, nazwiska pracowników, adresy e-mail, a nawet nazwy stosowane w systemie sieci korporacyjnej.
- Serwery DNS pozwalają na „transfer stref”, podając adresy IP, nazwy serwerów i adresy e-mail.

Niebezpieczna architektura sieci

Projekt architektury sieci ma podstawowe znaczenie dla właściwej segmentacji sieci na Internet, sieć korporacyjną firmy i sieć SCADA. Słabe punkty infrastruktury sieciowej zwiększają ryzyko, że włamanie z Internetu umożliwi penetrację systemu SCADA. A oto niektóre typowe słabe punkty architektury sieci:

- Konfiguracja serwerów FTP, sieci WWW i pocztowych, niekiedy niezamierzenie i niepotrzebnie, umożliwia dostęp do wewnętrznej sieci korporacyjnej.
- Połączenia sieciowe z partnerami firmy są zabezpieczane za pomocą zapory ogniowej, systemu wykrywania włamań lub systemów sieci VPN niezgodnych z innymi sieciami.
- Niepotrzebnie wydawana jest zgoda na dostęp modemowy, a przy dokonywaniu połączeń za jego pośrednictwem nie są przestrzegane obowiązujące w firmie reguły dotyczące dostępu telefonicznego.
- Zapory ogniowe i inne mechanizmy kontroli dostępu do sieci nie są stosowane wewnętrznie, przez co różne segmenty sieci są odizolowane od siebie słabo lub wcale.

Brak monitorowania w czasie rzeczywistym

- Pracowników działu zabezpieczeń informatycznych w firmach użyteczności publicznej przytłaczają ogromne ilości danych nadchodzące z urządzeń zabezpieczających sieć, co sprawia, że próby monitorowania stają się daremne.
- Nawet w firmach, w których wdrożono systemy wykrywania włamań, pracownicy działów zabezpieczeń sieci mogą wykrywać tylko poszczególne zdarzenia, a nie zorganizowane ataki, które układają się w incydenty widoczne dopiero w dłuższym przedziale czasu.

> Taktyka wzmocnienia zabezpieczeń systemu SCADA

Najskuteczniejsze strategie zabezpieczeń informatycznych dla firm użyteczności publicznej to połączenie systematycznych, okresowych analiz stanu zabezpieczeń oraz ciągłej uwagi poświęcanej architekturze zabezpieczeń i monitorowaniu. Poniżej podano najważniejsze kroki zmierzające w kierunku zmniejszenia liczby i wagi przypadków naruszenia zabezpieczeń.

KROK 1: SYSTEMATYCZNE ANALIZY STANU ZABEZPIECZEŃ

Wiele firm użyteczności publicznej nie dokonuje systematycznych, okresowych ocen stanu zabezpieczeń systemów SCADA i EMS (Energy Management Systems, systemy zarządzania energią). Należy wykonywać analizy stanu zabezpieczeń nie tylko systemów eksploatacyjnych, lecz również sieci korporacyjnych, serwerów sieci WWW i systemów zarządzania relacjami z klientami. Dzięki temu można ujawnić nieoczekiwane luki w zabezpieczeniach, takie jak nieznanne połączenia między sieciami publicznymi a prywatnymi oraz problemy z konfiguracją zapór ogniowych.

KROK 2: FACHOWY PROJEKT ARCHITEKTURY ZABEZPIECZEŃ INFORMATYCZNYCH

Firmy użyteczności publicznej mają do wyboru ogromną liczbę technologii zabezpieczeń, urządzeń sieciowych i opcji konfiguracji. Co prawda zapory ogniowe, systemy wykrywania włamań i sieci VPN są stworzone do ochrony sieci przed atakami, ale nieprawidłowa konfiguracja lub zły dobór środków zabezpieczających wystarczą, by drastycznie zmniejszyć skuteczność zabezpieczeń. Aby zmniejszyć zagrożenia związane z projektem architektury sieci, firmy użyteczności publicznej powinny konsultować się ze specjalistami w dziedzinie zabezpieczeń informatycznych. Pozwoli to wykluczyć przypadki obniżenia bezpieczeństwa wskutek wprowadzania zmian w architekturze sieci.

KROK 3: ZARZĄDZANIE ZABEZPIECZENIAMI

Im więcej urządzeń zabezpieczających stosują firmy w swoich sieciach, tym trudniejsze staje się właściwe zarządzanie tymi urządzeniami i ich nadzorowanie. Niestety, samo wdrożenie rozwiązań technicznych przy braku ścisłego nadzorowania i zarządzania znacznie zmniejsza skuteczność urządzeń zabezpieczających. Zatrudnienie doświadczonych fachowców w dziedzinie zabezpieczeń informatycznych do nadzoru nad urządzeniami zabezpieczającymi może zmniejszyć stopień zagrożenia. Ta możliwość jest jednak zbyt kosztowna dla większości, jeśli nie wszystkich firm użyteczności publicznej. Dlatego właśnie wiele organizacji zleca zarządzanie i nadzór nad urządzeniami zabezpieczającymi firmom wysoce wyspecjalizowanym w zarządzaniu zabezpieczeniami. Usługi zarządzania zabezpieczeniami zapewniają właściwą, aktualną konfigurację wszystkich urządzeń zabezpieczających, a zarazem monitorowanie w czasie rzeczywistym faktycznej aktywności urządzeń i błyskawiczne wykrywanie podejrzanych działań. Usługi zarządzania zabezpieczeniami pozwalają firmom korzystać z monitorowania bezpieczeństwa w czasie rzeczywistym przy względnie niskim koszcie, a jednocześnie zwiększyć wartość stosowanych urządzeń zabezpieczających dzięki pełnemu wykorzystaniu ich faktycznych możliwości.

FIRMA SYMANTEC – ŚWIATOWY LIDER W DZIEDZINIE TECHNOLOGII ZABEZPIECZEŃ INTERNETOWYCH – OFERUJE SZEROKI ZAKRES OPROGRAMOWANIA ORAZ URZĄDZEŃ ZABEZPIEZAJĄCYCH SIEĆ DLA UŻYTKOWNIKÓW INDYWIDUALNYCH ORAZ FIRM. FIRMA SYMANTEC JEST NAJWIĘKSZYM NA ŚWIECIE DOSTAWCĄ TECHNOLOGII OCHRONY ANTYWIRUSOWEJ, ZAPÓR OGNIOWYCH, WIRTUALNYCH SIECI PRYWATNYCH, ZARZĄDZANIA LUKAMI W ZABEZPIECZENIACH, WYKRYWANIA WŁAMAŃ, FILTROWANIA TREŚCI INTERNETOWYCH I ZAWARTYCH W POCZCIE ELEKTRONICZNEJ, ZDALNEGO ZARZĄDZANIA ORAZ USŁUG ZABEZPIEZAJĄCYCH DLA PRZEDSIĘBIORSTW. MARKA NORTON FIRMY SYMANTEC, KTÓRĄ OPATRZONE SĄ DETALICZNE WERSJE PRODUKTÓW ZABEZPIEZAJĄCYCH, JEST ŚWIATOWYM LIDEREM POD WZGLĘDEM SPRZEDAŻY DETALICZNEJ ORAZ ZDOBYWCĄ NAJWIĘKSZEJ LICZBY NAGRÓD PRZYZNAWANYCH PROGRAMOM KOMPUTEROWYM. CENTRALA ŚWIATOWA FIRMY ZNAJDUJE SIĘ W CUPERTINO W KALIFORNII, USA, A JEJ FILIE DZIAŁAJĄ W 38 KRAJACH NA CAŁYM ŚWIECIE.

WIĘCEJ INFORMACJI MOŻNA ZNALEŹĆ NA STRONIE [HTTP://ENTERPRISESECURITY.SYMANTEC.COM](http://ENTERPRISESECURITY.SYMANTEC.COM)

CENTRALA ŚWIATOWA
20330 Stevens Creek Blvd.
Cupertino, CA 95014 U.S.A.
+ 1 408 517 8000
+1 800 441 7234

SYMANTEC (POLSKA)
Al. Jana Pawła II 29
00-867 Warszawa
Tel. (22) 586 92 00
Faks (22) 654 69 69
www.symantec.pl

Firma Symantec ma biura w 38 krajach. Informacje o biurach i numery telefonów dla poszczególnych krajów można znaleźć w naszej witrynie internetowej: www.symantec.com

Informacje dotyczące obsługi klientów i pomocy technicznej można znaleźć w naszej witrynie internetowej: www.symantec.com/eusupport