Dr inż. Krzysztof Billewicz
Instytut Energoelektryki
Politechnika Wrocławska

Bezpieczeństwo cyfrowe firm energetycznych. Czy pierwsze przyczółki obrony mogą zostać łatwo zdobyte?

Digital safety of electric power companies. Can the first defence bridgeheads be easily captured?

Bardzo często zdarza się, że pracownicy nie czytają regulaminów zakładowych ani zasad bezpieczeństwa w szeroko pojętej cyberprzestrzeni. Nawet, jeżeli zapoznają się z nimi z konieczności, to nierzadko bywa, że dość szybko zapominają o podstawowych zasadach. Koncentrują się na obowiązkach służbowych. Zdaniem niektórych badaczy pracownicy są zbyt przepracowani albo zbyt leniwi, aby trzymać się takich zasad. To z kolei powoduje, że nie znając zasad bezpieczeństwa nierzadko narażają samych siebie i sieci komputerowe w przedsiębiorstwach na różnego rodzaju ataki cyberprzestępców. Taka ignorancja zasad bezpieczeństwa w pracy powoduje, że pracownicy koncernów energetycznych mogą narażać na szwank funkcjonowanie krajowego systemu elektroenergetycznego. W takim przypadku straty finansowe mogą być ogromne.

Ataki mogą być fizyczne, jeżeli jest to dobre określenie na prowadzenie działalności w cyberprzestrzeni, zewnętrzne (np. wejście do siedziby przedsiębiorstwa i kradzież sprzętu, danych lub dostanie się do sieci przedsiębiorstwa po wewnętrznej stronie firewalla) oraz socjotechniczne.

Wielu ludzi żyje w złudnym przeświadczeniu o swojej odporności na ataki cybernetyczne, twierdząc i uważając, że są zbyt sprytni, żeby ktoś manipulował nimi, oszukiwał ich albo wywierał na nich wpływ. Zakładają, że takie sytuacje zdarzają się tylko osobom naiwnym i głupcom [1] albo w filmach.

Bezpieczna cyberprzestrzeń przedsiębiorstw energetycznych staje się elementem koniecznym do prowadzenia niezawodnej pracy systemu elektroenergetycznego. A taka praca jest warunkiem zapewnienia bezpieczeństwa narodowego. W związku tym dotyka się bardzo krytycznych aspektów. Bezpieczeństwo narodowe nie powinno być zagrożone tylko dlatego, że niektórzy pracownicy (lub dostawcy oprogramowania) nie stosują podstawowych zasad bezpieczeństwa cyfrowego.

W artykule opisano najprostsze metody pokonania przez cyberprzestępcę pierwszej linii w dostępie do sieci informatycznej przedsiębiorstwa. Artykuł napisany jest w celu przeprowadzenia kontroli wszystkich ważnych aplikacji w przedsiębiorstwach energetycznych oraz szczególnego uczulenia pracowników na występujące zagrożenia. Opisane poniżej przypadki pokazują, jak proste może być pokonanie pierwszej linii obrony i uzyskanie pewnych danych, które cyberprzestępcy mogą wykorzystać do dalszej penetracji firmowych sieci komputerowych.

Polityka haseł pracowników

Prawie każdy pracownik przedsiębiorstwa energetycznego musi pamiętać bardzo wiele haseł [2]. Najczęściej występujące hasła angielskie są bardzo proste:

- 123456 – wszelkie kombinacje od 12345 do 1234567890,
- Password,
- Iloveyou,
- Princess,
- abc123,
- 111111,
- 123.456 oraz
- dla użytkownika ‘admin’ hasła ‘admin’, ‘admin123’ albo ‘admin12345’.

Co więcej, często wymuszona jest okresowa zmiana hasła oraz zakłada się, że używane hasła nie mogą być zbyt proste. W konsekwencji po kolejnej zmianie hasła pracownik przestaje panować nad własnymi hasłami dostępowymi. Dlatego albo wprowadza jedno hasło (wg niektórych oszacowań ponad 60% pracowników używa jednego hasła do logowania się w więcej niż jednej aplikacji), identyczne do wszystkich aplikacji albo zapisuje je w pliku lub na łatwo dostępnej kartce papieru. Taka kartka najczęściej znajduje się w podręcznej szufladzie, na górnej półce albo przy komputerze. Czasami na monitorze przyklejona jest kartka z obecnym hasłem logowania do systemu.

Wykorzystywanie identycznego hasła do logowania się do różnych programów, aplikacji i portali internetowych ułatwia przeprowadzenie ataku. Łatwość wynika z tego, że po pewnym czasie pracownik przestaje panować nad tym, w ilu portalach podał swoje jedyne hasło.

Atak może przebiegać w opisany poniżej sposób.

1. Napastnik tworzy stronę www, informującą, że można wygrać określoną sumę pieniędzy, nowoczesnego laptopa lub smartfona. Stronę taką reklamuje wysyłając wiadomości e-mail lub reklamuje ją na portalu społecznościowym. Warunkiem zdobycia nagrody jest jedynie wypełnienie krótkiej i prostej ankiety. Aby wypełnić ankietę na takich stronach www należy stworzyć własne konto i następnie zalogować się podając swój adres e-mail. Pracownik tworzy konto na tym portalu, podając swojego e-maila oraz swoje hasło,

które najprawdopodobniej jest również jego hasłem wykorzystywanym podczas logowania do serwera pocztowego, konta bankowego itp.

2. Aby uwiarygodnić takie strony często zamieszczony jest tam napis: *nikomu nigdy nie podawaj swojego hasła*. Oczywiście użytkownicy wiedzą o tym, natomiast takie oczywiste sformułowania usypiają czujność użytkowników. Oczywiście czas ważności takiego hasła, zdobytego przez cyberprzestępcę, jest krótki i napastnik musi się spieszyć. W każdym razie pracownik dobrowolnie podaje napastnikowi namiary na pierwsze miejsce do nieupoważnionego dostępu. Napastnik dostając się na serwer pocztowy nierzadko może znaleźć tam informacje o sposobie zalogowania do niektórych portali, ponieważ czasami po utworzeniu tam konta nowy użytkownik otrzymuje e-maila zwrotnego, w którym są informacje: login i hasło dostępowe do różnych aplikacji i systemów.

Polityka haseł dostępowych do urządzeń

W obszarze polityki haseł niebagatelną sprawą staje się przechowywanie haseł. W przedsiębiorstwie energetycznym, oprócz milionów liczników, będzie również wykorzystywana niezliczona ilość urządzeń elektronicznych, do których trzeba będzie podawać hasło. W przedsiębiorstwie muszą być zawsze dostępne informacje na temat obecnych haseł, dlatego dodatkowo pojawiają się problemy przechowywania takiej ilości haseł, ponieważ każdy pracownik może w dowolnym momencie rozwiązać stosunek pracy. W szczególnych przypadkach może on odejść z pracy z dnia na dzień i np. wyjechać do innego kraju. Koniecznością staje się z jednej strony umożliwienie dostępu uprawnionych pracowników do zbioru haseł, z drugiej natomiast ograniczenie dostępu jedynie do grona osób uprawnionych.

W przypadku zarządzania hasłami dochodzi kwestia okresowego ich zmieniania w urządzeniach, odpowiedniego dokumentowania takiego faktu, opracowanie metod postępowania w przypadku stwierdzenia pomyłek itp. Pracownicy, którzy pożegnali się z firmą, mogli zapamiętać lub zarejestrować hasła do dowolnych urządzeń, a taka wiedza mogłaby umożliwić lub ułatwić włamanie do sieci przedsiębiorstwa. Fakt ten jednak nie będzie znany.

Dodatkowo podkreśla się fakt, że korzystanie z jednego konta (np. konto operator, które wykorzystują wszyscy pracownicy) przez wielu użytkowników przy zmianach konfiguracji danego urządzenia powoduje, że po pewnym czasie nie można określić, np. kto skonfigurował urządzenie w nieprawidłowy sposób.

Należy również pamiętać, że po zainstalowaniu jakichkolwiek nowych urządzeń w przedsiębiorstwie wszystkie domyślne hasła muszą zostać zmienione. Hasła nie mogą być zbyt łatwe do odgadnięcia.

Modyfikacja zapytań SQL

SQL Injection (z ang., dosłownie zastrzyk SQL) – luka w zabezpieczeniach aplikacji internetowych (i nie tylko), polegająca na nieodpowiednim filtrowaniu lub niedostatecznym typowaniu i późniejszym wykonaniu danych przesyłanych w postaci zapytań SQL do bazy danych. Ten typ ataków wykorzystuje nieodpowiednie filtrowanie znaków ucieczki z danych wejściowych, co pozwala na przekazanie dodatkowych parametrów do zapytania. W wyniku odpowiednio spreparowanego polecenia do bazy danych haker pobierze z bazy danych wszystkie rekordy zamiast jednego wybranego.

Aplikacja (np. strona www) prosi o podanie nazwy użytkownika – LOGIN oraz hasła – PASSWORD. Następnie w bardzo prosty sposób tworzone jest zapytanie do bazy danych, które pozwala uzyskać rekord dotyczący tego użytkownika. W programie zaszyte jest puste zapytanie, gdzie pola LOGIN i PASSWORD uzupełniane są dokładnym tekstem wpisanym przez użytkownika:

```
SELECT * FROM users WHERE (name ='LOGIN')
AND (haslo='PASSWORD');
```

Zapytanie to mówi – wyciągnij z bazy wszystkie rekordy, w których spełnione są warunki, że name ='LOGIN' oraz haslo ='PASSWORD'.

Takie rozwiązanie działałoby prawidłowo, gdyby nie możliwość wpisania jako nazwę użytkownika lub hasło fragmentu kodu SQL. Przykładowo wpisanie jako hasło niepozornego tekstu 'OR '1'= '1 powoduje diametralną zmianę znaczenia zapytania kierowanego do bazy danych.

```
SELECT * FROM users WHERE (name ='LOGIN')
AND (haslo=''OR '1'= '1');
```

W konsekwencji otrzymuje się zapytanie: Wyciągnij z bazy danych rekordy, w których nazwa użytkownika jest name= 'LOGIN' oraz dokonywana jest suma logiczna warunków: haslo='' warunek nigdy nie jest spełniony oraz warunku '1'='1', który zawsze jest spełniony. Zatem w takim przypadku

Haker może wpisać jako nazwę użytkownika ciąg znaków: LOGIN') -- co spowoduje, że wynikowe zapytanie do bazy danych będzie następujące:

```
SELECT ID FROM USERS WHERE (name ='LOGIN') --')
AND (haslo='');
```

W składni SQL to co znajduje się po dwóch myślnikach umieszczonych obok siebie, to komentarz, więc będzie to fragment pomijany. Czyli można będzie uzyskać pewne dane z bazy danych bez wpisywania hasła.

W obydwu opisanych wcześniej przypadkach haker może zalogować się do bazy na konto administratora, bez znajomości jego hasła.

Istnieje cały szereg komend, które napastnik może wykorzystać w celu przeprowadzenia złośliwego działania. Przykładowo może on wpisać jako nazwę użytkownika sekwencję:

```
'); DELETE FROM USERS --
```

która spowoduje wykasowanie zawartości tabeli z listą użytkowników (przy założeniu, że haker zna nazwę tej tablicy).

Jeżeli napastnik zna nazwę bazy danych, to może nawet pokusić się o jej bezpowrotne wykasowanie wpisując, jako nazwę użytkownika:

'); DROP DATABASE SKLEP --

Oczywiście w niektórych przypadkach, aby skutek zmian (wykasowania elementów z bazy danych) zaistniał, konieczne jest potwierdzenie prawidłowości polecenia przy użyciu rozkazu: COMMIT. Polecenie to potwierdza zmiany wykonane w bieżącej sesji (bieżącym połączeniu z bazą danych). Dopóki nie zostaną potwierdzone zmiany pozostali użytkownicy nie mają dostępu do zmienionych danych. Widzą dane przed zmianami. Korzystając z ataku typu SQL Injection można również przeprowadzić atak typu DoS (odmowy usługi).

Są dwie główne przyczyny błędów typu SQL Injection:

- niewystarczająca walidacja danych wejściowych lub jej brak;
- brak kodowania znaków specjalnych przed wstawieniem do zapytania SQL.

Podstawową konsekwencją takiego błędu może być ujawnienie, modyfikacja lub usunięcie danych przechowywanych w bazie.

Podstawowym sposobem zabezpieczania przed atakiem typu SQL Injection jest niedopuszczenie do nieuprawnionej zmiany wykonywanego zapytania. Odpowiednie zabezpieczenia przed skutkami wykonania błędnych zapytań, które mimo wszystko dostaną się do bazy, mogą również znajdować się na poziomie bazy danych. Aby zapobiec tego typu atakom, należy traktować wszystkie dane otrzymywane z zewnątrz jako niezaufane i sprawdzać ich poprawność.

Bezpieczeństwo kopii zapasowych

Ponieważ czasami zdarzają się awarie systemów informatycznych, pojedyncze osoby oraz przedsiębiorstwa starają się tworzyć i przechowywać kopie danych. Nierzadko zdarza się, że tworzonych jest wiele kopii danych i pracownik przestaje już panować nad tym, w jakim miejscu przechowywana jest jaka kopia. Pierwszym symptomem pokazującym, że konieczne jest uporządkowanie kopii jest kończące się miejsce na dysku komputera, serwera lub urządzenia rezerwowego [1].

Zauważono jednak, że tak jak zabezpiecza się systemy oraz oryginalne dane i informacje, tak kopie bezpieczeństwa nierzadko nie podlegają praktycznie żadnej ochronie lub chronione są bardzo słabo. Przedsiębiorstwo zatem skupia się na tym, aby chronić i dostarczać pewne dane, natomiast kopie tych danych traktowane są jako nieważne. Czasami taśmy z kopiami przechowywane są w pudełku, dostępnym dla wielu pracowników, a czasem również dostęp ma firma zewnętrzna świadcząca jakieś usługi dodatkowe [1] lub osoba przechodząca przez dane biuro.

W książce [1] opisana jest sytuacja, w której ważny pracownik działu IT pewnej firmy przechowywał kopie zapasowe wielu swoich plików i dokumentów. Wśród nich znajdowała się kopia wszystkich e-maili i kontaktów. I taka kopia dostała się w ręce hakera. Ten znalazł w niej wiele ciekawych informacji. Dowiedział się z poczty elektronicznej o prywatnych sprawach pracownika, jego podejściu do pracy, informacjach, którzy pracownicy za co odpowiadają. Było tam również kilka e-maili potwierdzających utworzenie konta na serwerze, z informacją, jak może się tam zalogować wraz z loginem i hasłem. Podobne e-maile były przez niego wysłane do firm zewnętrznych, które potrzebowały łączyć się z siecią przedsiębiorstwa.

Czasami kopie przechowywane są na niezabezpieczonych urządzeniach przenośnych: pamięciach USB – pendrive'ach, dyskach zewnętrznych, taśmach, płytach CD i DVD itp. Nierzadko takie urządzenia znajdują się w chaosie ma biurkach lub na półkach, skąd każdy przechodzący mógłby je zabrać. Czasami zdarzają się kradzieże laptopów, komputerów stacjonarnych lub samych ich dysków pamięci. Autor artykułu trzykrotnie spotkał się z przypadkiem kradzieży laptopa różnym pracownikom przedsiębiorstwa IT tworzącego oprogramowanie dla elektroenergetyki: wyniesionego z siedzimy przedsiębiorstwa IT, zostawionego w hotelu, podczas włamania do zaparkowanego samochodu służbowego. Natomiast nieznany jest żaden przypadek jakiegokolwiek wykorzystania danych i informacji przechowywanych na tych skradzionych komputerach.

Zakończenie

Okazuje się, że w zakresie bezpieczeństwa cyfrowego bardzo ważne jest podejście pracowników. Należy podjąć wszelkie kroki, aby ograniczyć ignorancję w tym obszarze, oczywiście jeżeli ona występuje.

Warto już teraz testowo przebadać WSZYSTKIE aplikacje wykorzystywane w przedsiębiorstwie energetycznym na okoliczność wstrzykiwania komend SQL jako nazwy użytkownika lub hasło. Lepiej to zrobić teraz świadomie i pod kontrolą niż czekać, aż cyberprzestępca zrobi to w najmniej spodziewanym momencie, zagrażając stabilnej pracy systemu elektroenergetycznego.

Należy uczulić pracowników przed zakładaniem kont na tajemniczych stronach www oraz podkreślić, że nie mogą podawać tam służbowego e-maila.

Nierzadko podkreśla się fakt, że w elektroenergetyce pracuje wiele osób – wybitnych elektroenergetyków, którzy mają jednak bardzo małe pojęcie w zakresie bezpieczeństwa cyfrowego.

Ogólnie, w wielu krajach problemem jest starzejąca się siła robocza w przedsiębiorstwach energetycznych, z której duża część pracowników przejdzie na emeryturę w ciągu najbliższych 5 - 10 lat. Przedsiębiorstwa energetyczne będą mogły zapełnić lukę talentami młodych ludzi, którzy będą w stanie zbudować inteligentną sieć elektroenergetyczną przyszłości [3]. Dla niektórych, dotychczasowych pracowników problematyka związana z zastosowaniem najnowszych technologii teleinformatycznych nierzadko może być bardzo dużym wyzwaniem. Podobnie jest z bezpieczeństwem cyfrowym, którego zapewnienie staje się coraz ważniejszym warunkiem prawidłowo realizowanych dostaw energii do odbiorców końcowych.

PIŚMIENNICTWO

[1] Mitnick K. D., Simon W.L., The art of intrusion. The real stories behind the exploits of hackers, intruders and deceivers, 2005. Polskie wydanie: Sztuka infiltracji, czyli jak włamać się do sieci komputerowych, Wydawnictwo A. Kuryłowicz, Warszawa 2006.

[2] Billewicz K., Problematyka bezpieczeństwa informatycznego w inteligentnych sieciach, Konferencja APE 2011, T.2, s. 115-120.

[3] Substation Automation for the Smart Grid, White Paper, cisco, 2010 Cisco.