S-Cabling

SIEMON™
CABLING SYSTEM

Systemy bezpieczeństwa transmisji danych rządowych udoskonalone dzięki systemowi okablowania TERA

To, że sprawy bezpieczeństwa IT są gorącym tematem, nikogo nie dziwi. Kwestie bezpieczeństwa zaprzątały od zawsze umysły szefów działów IT, natomiast w sektorze prywatnym obserwowany ostatnio napływ informacji, uregulowań i produktów związanych z bezpieczeństwem sieci jest pewną nowością. Nie tak jak w sieciach rządowych czy wojskowych. Te sieci o krytycznym znaczeniu od dawna na czele swych list umieszczały bezpieczeństwo, a podejście takie przyniosło w rezultacie niezmiernie surowe parametry i procedury dotyczące bezpieczeństwa.

W sektorze prywatnym, bezpieczeństwo informacji oparte jest zazwyczaj na takich środkach, jak firewalls, hasła, biometria czy karty dostępu. Informacje rządowe, w tym informacje departamentu obrony, dane ochrony zdrowia czy informacje infrastruktury gmin, są często chronione przez podobne systemy. Poziom bezpieczeństwa wyznaczany jest przez charakter danych. W bardziej chronionych/zastrzeżonych sieciach rządowych, środki bezpieczeństwa obejmują warstwę fizyczną instalacji kablowej.

Wdrożenie zabezpieczenia warstwy fizycznej przebiega w kilku etapach. Pierwszym i najważniejszym jest udokumentowanie i oznakowanie warstwy fizycznej. Ważne jest, by znać każdy punkt wejścia i wyjścia w sieci. Bez tej informacji bezskuteczne mogą okazać się wszelkie dodatkowe kroki podejmowane w celu wykrycia punktu naruszenia sieci. Dokumentację warstwy fizycznej można sporządzić drogą inteligentnego krosowania (inteligent patching), metodami ręcznymi lub przez połączenie obu sposobów. Sektor prywatny chętnie wdraża takie działania, które stają się w coraz większym stopniu częścią zarządzania siecią w instytucjach pozarządowych.

Kiedy infrastruktura sieci jest już właściwie udokumentowana, kolejnym krokiem na drodze do bezpieczeństwa fizycznego jest sprawdzenie przebiegów kablowych i przestrzeni w celu zapewnienia, że kabel jest niedostępny dla nieupoważnionego personelu. Oprócz ograniczenia dostępności fizycznej, należy też kontrolować sygnały radiacyjne instalacji kablowej.

Sygnały radiacyjne lub emisje występują w każdym elemencie wyposażenia komputerowego. W Stanach Zjednoczonych, Federalna Komisja ds. Komunikacji (FCC) kontroluje ilość dozwolonych emisji; istnieją też jej międzynarodowe odpowiedniki (dokumenty IEC CISPR). Ta niepożądana różnorodność emisji sygnałów określana jest jako przypadkowe przekazywanie sygnałów odnoszących się do tajnych informacji. Emisje takie mogą być przekazywane przez linie energetyczne, kable przesyłu danych lub po prostu przez promieniowanie sygnału. Kiedy taki przypadkowy przekaz zostanie odebrany, zagrożone jest bezpieczeństwo informacji. Krótko mówiąc, każdy element urządzenia przetwarzającego dane, łącznie z mikroukładami, diodami i tranzystorami, jest potencjalnym źródłem przypadkowego przekazywania sygnałów.

Kontrola oraz/lub eliminacja wszystkich źródeł przypadkowego przekazywania sygnałów ma kluczowe znaczenie w przypadku komunikacji rządowej, która wymaga wysokiego poziomu bezpieczeństwa, np. informacje dotyczące spraw wewnętrznych. Podlega to takim rządowym określeniom, jak EMSEC, INFOSEC oraz TEMPEST. Programy te funkcjonują w celu zapewnienia, że normalne sygnały radiacyjne są w określony sposób chronione przed niesumiennymi słuchaczami, którzy mogliby wykorzystać przechwycone informacje dla niewłaściwych celów.

TEMPEST to słowo-kod rządu amerykańskiego, które określa normy opracowane w celu ochrony transmisji danych przed elektronicznym szpiegostwem. Mimo iż rzeczywiste wymogi są zastrzeżone, ogólnie wiadomo, że TEMPEST wyznacza ścisłe limity w zakresie promieniowania sygnałów z elektronicznych urządzeń przetwarzania danych. Podczas gdy zakres opublikowanych informacji TEMPEST skupia się na wyposażeniu fizycznym, takim jak monitory, drukarki czy urządzenia zawierające mikroukłady, określenie to jest powszechnie stosowane w odniesieniu do działań w zakresie bezpieczeństwa emisji (EMSEC). EMSEC oznacza w rozumieniu komitetu ATIS TIAI, „ochronę wynikającą ze wszelkich środków przeznaczonych do uniemożliwienia uzyskania przez nieupoważnione osoby jakichkolwiek informacji, które mogą być pozyskane z odbioru i analizy przypadkowych sygnałów spoza systemów telekomunikacyjnych czy urządzeń szyfrujących".

TEMPEST zaczął działać wiele lat temu, kiedy okazało się, że można wykryć transmisje drogą powietrzną z dużej odległości poprzez nasłuch emisji z kabla. W 1918 roku, Herbert Yardley oraz jego zespół tzw. „Black Chamber" został zatrudniony przez armię amerykańską w celu opracowania metod wykrycia, odbioru i wykorzystania telefonów bojowych oraz ochrony nadajników radiowych. Niemniej jednak, do lat 60-tych i 70-tych ubiegłego wieku nie stosowano określenia TEMPEST. Istnieje obecnie kilka definicji tego skrótu, np. „Telekomunikacyjno-elektroniczny materiał chroniony przed emisją fałszywych transmisji" czy „Norma dotycząca przekazywania nieustalonych impulsów elektromagnetycznych". Powyższe próby rozwinięcia skrótu TEMPEST są tylko przypuszczeniami, ponieważ oficjalna nazwa, razem z jej aktualnymi wymogami, ma charakter zastrzeżony. W skrócie, TEMPEST to środki służące ochronie transmisji i obejmuje media, urządzenia komunikacyjne oraz inne działania ochronne. Podstawowe wymogi i protokoły TEMPEST zostały ujawnione w 1995 r. jako NSTISSAM TEMPEST. Mimo iż te dokumenty obrazowały część metodologii TEMPEST, faktyczne limity emisji oraz parametry testowe zostały zmienione i pozostają zastrzeżone. Nawet bez bardziej szczegółowych parametrów, TEMPEST służył jako model dla wielu innych podobnych programów rządowych. Odpowiednikiem w NATO jest program AMSG 720B. W Niemczech, mimo iż nazwy norm określanych przez rząd pozostają zastrzeżone, jest rzeczą wiadomą, że Krajowa Rada Telekomunikacyjna zarządza programem podobnym do TEMPEST. W Wielkiej Brytanii z kolei, własny program posiada Centrala Komunikacji Rządowej (GCHQ), odpowiednik amerykańskiego NSA (Zarządzanie Bezpieczeństwem Narodowym).

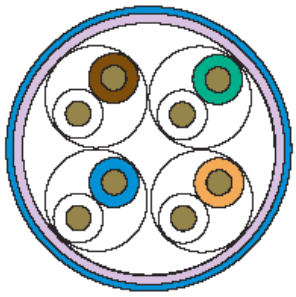
W Stanach Zjednoczonych, urządzenia spełniające normy TEMPEST są kategoryzowane według 3 poziomów aprobat. Aprobata typu 1 jest dopuszczona do stosowania w odniesieniu do zastrzeżonego lub kontrolowanego sprzętu kryptograficznego i może dotyczyć zespołów, komponentów lub innych elementów zatwierdzonych przez NSA dla zabezpieczenia telekomunikacji oraz zautomatyzowanych systemów dla ochrony zastrzeżonej lub wrażliwej informacji rządu amerykańskiego i jego partnerów. Taki sprzęt podlega restrykcjom zgodnie z przepisami International Traffic in Arms. Aprobata typu 2 przeznaczona jest dla sprzętu, zespołów i komponentów używanych do transmisji niezastrzeżonych, ale wrażliwych informacji. Typ 3 wdraża niezastrzeżony algorytm zarejestrowany w Krajowym Instytucie Norm i Technologii (NIST) do stosowania w ochronie niezastrzeżonej wrażliwej lub komercyjnej informacji. Podczas gdy sprzęt jest aprobowany indywidualnie, amerykańska certyfikacja TEMPEST odnosi się do całego systemu. W odniesieniu do sieci obejmuje to wszystkie komponenty, łącznie z instalacją kablową. Zmiana jednego komponentu może wpłynąć na bezpieczeństwo całego

systemu. W bezpiecznej komunikacji, medium używane do transmisji danych (np. okablowanie) jest częścią systemu TEMPEST lub EMSEC. Normy kontroli emisji TEMPEST dla okablowania, w połączeniu z szyfrowaniem danych oraz innymi systemami bezpieczeństwa, umożliwiają Bezpieczeństwo Informacji, INFOSEC. Ze względu na te niezmiernie surowe wymogi, rząd miał niewiele opcji do wyboru dla zapewnienia bezpieczeństwa warstwy fizycznej.

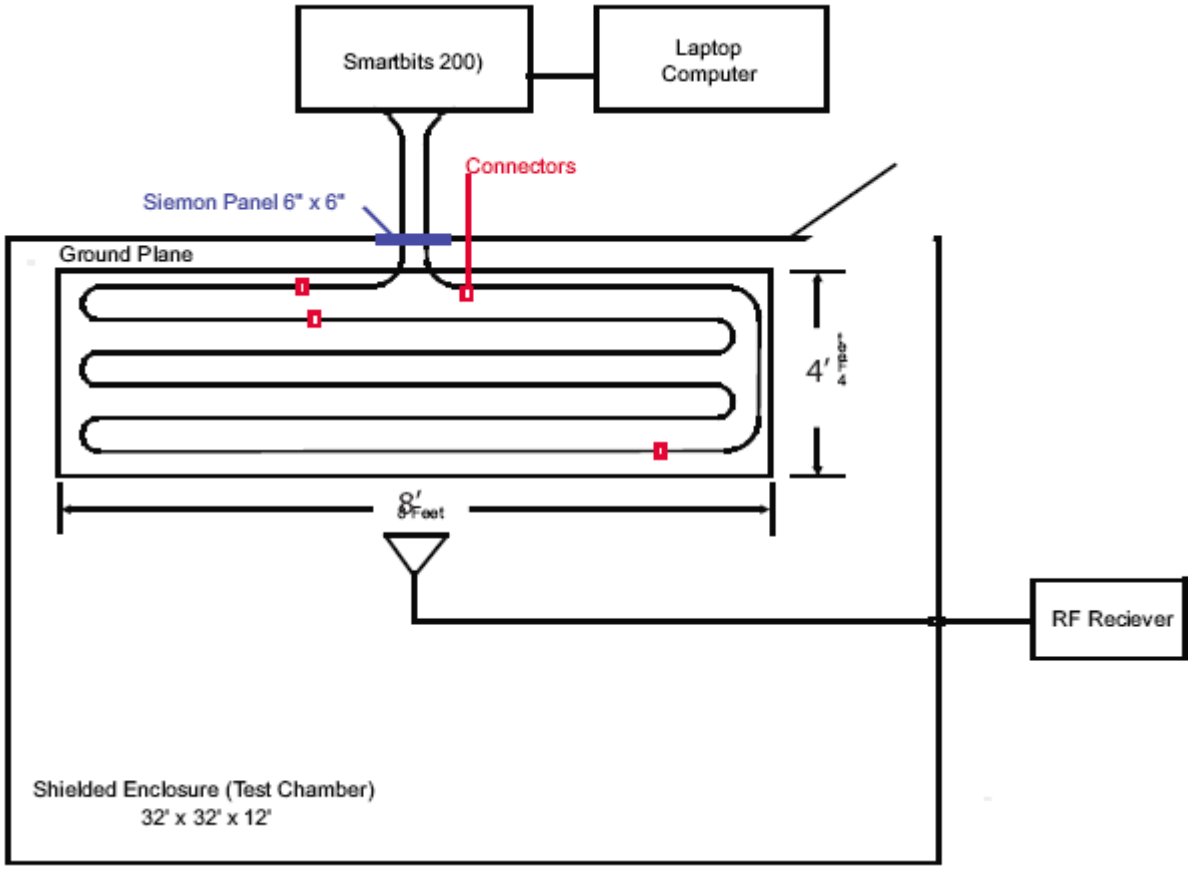
Jedną z możliwości było zastosowanie sieci światłowodowych. Okablowanie światłowodowe generuje tylko emisje ciepła. Dostarczało to dodatkowej ochrony ze względu na fakt, że włókno światłowodowe musiałoby być uderzone lub dotknięte wykrywaczem ciepła, żeby „szpiegować" komunikację. Wyposażenie sieci światłowodowej jest jednak bardziej kosztowne niż miedzianej.

Sieci miedziane były dopuszczalne, ale wymagały bardzo specyficznych praktyk instalacyjnych. Zgodnie z normami TEMPEST, w sieciach rządowych o wysokim poziomie bezpieczeństwa, potencjalnym emisjom zapobiega się poprzez umieszczanie wszystkich kabli w żelaznych kanałach. Oprócz kanałów, normy TEMPEST określiły też wytyczne rozdziału CZERWONY/CZARNY. Rozdział ten polega na tym, że instalacja kablowa i obszary pracy są podzielone na CZERWONE i CZARNE strefy. Stefy czerwone przenoszą informacje zastrzeżone i są izolowane oraz osłonięte przed strefami czarnymi przenoszącymi niezastrzeżone informacje. Strefy te są poddawane dalszym restrykcjom w zależności od ich umiejscowienia względem dostępu zewnętrznego, jak również odległości od innych potencjalnych źródeł promieniowania sygnału. W strefach czerwonych zakazane jest używanie sprzętów, takich jak telefony komórkowe i radia, które mogłyby nasłuchiwać lub przenosić sygnały. Ekranowany kabel miedziany dostarczał dodatkową warstwę zabezpieczenia, ograniczając część emisji, jednak pojedyncze całościowo ekranowane kable (FTP) nie eliminowały potrzeby stosowania kanałów oraz rozdziału na strefy czerwone i czarne w środowiskach o wysokim poziomie bezpieczeństwa. W przypadku kabli ekranowanych odległości przy rozdziale są mniejsze, co obniża koszt torów transmisyjnych i przestrzeni.

Najnowsze testy jednak przyniosły dodatkową opcję w zakresie sieci miedzianych dla połączeń z urządzeniami TEMPEST. TERA firmy Siemon, system kategorii 7/klasy F jest pierwszym systemem okablowania miedzianego, który przeszedł pozytywnie testy emisji TEMPEST w niezależnym, certyfikowanym przez NSA, laboratorium Dayton T. Brown Inc. TERA wykorzystuje kabel S/FTP oraz umożliwia w pełni ekranowaną dołączalność systemu. W kablu S/FTP każda para jest indywidualnie ekranowana, a wszystkie przewody otacza całościowa osłona ekranowana, jak pokazano na rysunku poniżej. Dodatkowe ekranowanie jest zintegrowane z wtyczkami sieciowymi, eliminując potencjalne źródła emisji.



Na potrzeby testu TEMPEST, 4-przewodowy, 100-metrowy kanał TERA został umieszczony w ekranowanej komorze bezechowej, jak pokazano na poniższym wykresie. Kanał został zasilony pełnym podwójnym ruchem Gigabit Ethernet (1000 Mb/s) wykorzystującym wieloportowy system analizy Spirant Smarbits. Emisje z systemu okablowania były następnie monitorowane oraz porównywane z wymogami TEMPEST.



Jak wynika z raportu z niezależnego testu, system TERA jest odpowiedni do zastosowań takich jak TEMPEST, w których dużą uwagę przykłada się do przypadkowego przekazywania sygnałów. Pozostała część raportu z testu ma charakter zastrzeżony.

Opracowanie: S-Cabling na podstawie materiałów z firmy SIEMON