Wyklad1

Saturday, January 8, 2022 8:40 AM

PERA - referencyjny model, który wprowadza podzial roznych komponentow i urzadzen ssieci przemyslowej na poziomy o wyzznaczonych funkcjach: podzial na poziomy 0-5

4-5 = - w praktcy jeden, siec przedsiebiorstwa(5), a 4kta to fragmenty sieci dot. zarzadzania

Pomiedzy 0-3 a 4-5 znajduje się strefa I-DMZ (industial demilitarized zone)
0-3 -> czesc produkcyjna i procesy z nia zwiazane

3 - systemy zarzadzania i monitorowania procesow calego zakladau. Min. MES
2 - systemy kontroli i monitorowania i sterowania produkcja ze posrednictwem komponentow
1 - inteligentne urzadzenia sterujace, steruja one i monitoruja komponentami z poziomu 0, Należy do nich min. SIS, PLC, RTU, IED
0 - obejmuje fizyczne komponenty, które sa pod kontrola i wykonuja faktyczna prace m.in.. Rozne sensory, czujniki, zawory, pompy czy silowniki

HMI - sluzy do nadzorowania jakis komponentow blizej tych tychze komponentow (np. jakis mikro monitorek konkretnego urzadzenia, gdy SCADA jest bardziej makro)

MES - pobieraja informacje i maja dostarczyc informacji biznesowej, np. dane historyczne, np. czy jakies komponenty nie będą do wymiany etc, można to tez podpiac potem pod raportowanie etc

Strefa srodowiska - definiuj eubior ochronny i wszelkie bariery i bezieczne odstepy

OT - operational tech
ICS - industrial Control System

OT - kkomponenty fizyzne jak np. czujniki czy jakies inne urzadzenia do zbierania danych:
- zawory i pompy
- kamery/termostaty
- maszyny, roboty
- czujniki wilgotnosci, ruchu
- pomiar zasilania, predkosci

ICS - do tego będą nalezec tego typu rozwiazania jak SCADA. To sa systemy do montorowania OT (wykorzystuja ich dane)

SCADA - potrzebne do:
- aby personel zakladu wiedzial co się dzieje
- automatyzacja i podejmowanie decyzji na podstawie tych monitorow (ogolnie zarzadzanie)

PLC i RTU - mniej wiecej podobny cel. PLC - stosuje się do oprogramowania procesu na podstawie danego stanu. Roznica - plc wymaga wiedzy bardziej niskopoziomowej, szersza funkcjonalnosc. Rtu - jest bardziej specjalistyczne pod dane zastosowanie, `nie da się okodowac wszystkiego, dostosowane pod proces,

IED - pobiera dane, przetwarza i transmituje dalej - taki ELT

DCS - rola tego i SCADA sa bardzo podobne. DCS - sa bardziej rozwiazania specjalistyczne pod klucz, ukierunkowe pod dana czynność, zawiera komponenty poziomu 0,1. Rozwiazania wlasnosciowe danych firm. Dedykowane pod dana firme. Scada pod dana firme/proces. SCADA jes duzo bardziej otwarta.

MES i HISTORIAN
Mes - dziala na poziomie 3, wiec ponad SCADA czy DCS. System do podejmowania decyzji. On tez przechowuje ogrom danych jak historian, i powoli się to integruje (jeden z drugim) mes jest duzo szerszy
HISTORIAN - gromadzi dane historyczne, poziom 3

HMI - umozliwia pracownikom weryfikacje i zmiane konfiguracji lokalnych procesow (blisko maszyn)

SIS - glowny cel , jeżeli zachodza zdarzenia krytyczne to przerwac i wyizolowac to zdarzenie. Glownym celem jest ochrona pracownikow, srodowiska itp. - to nie ma duzego zwiazku z cybersecurity, bardziej ochrona fizyczna procesow

Elemtry tworzace insrastrukture przemyslowa (OT) - Iot gateways, industrial wireless, industrial security appliance, industrial switching, industial routing

Przyklady i zastosowania przemyslu

1. Dostawa mediow (np. mierzenie zuzycia wody zdalne, monitorowanie wyciekow, AMI(pomiar zuzycia energii elektrycznej), pomiar jakosci wody, VVO - optymalizacja poziomu napiecia, FLISR(Fault Location, isolation, service restorian0 - zdalnie, Utility WAN, public/private LTE FAN, Wi-SUN FAN, LoRa WAN, Heterogeneous FAN, wymagana jest komunikacja wszystkiego np. miedzy personelem i urzadzeniami (+tu jest istotna cybersecurity), ogromny teren - identyfikacja zasobow
2. Produkcja przemyslowa - lancuch dostaw (obsluga magazynu, zarzadzanie zapasami, mobilnosc przemyslowa, sledzeni ezasobow), produkcja - automatyka przemysl, gromadzenie i obsluga danych, widocznosc i kontrola zasobow, zdalna obsluga. Ulatwienia w pracy - sprawna wymiana informacji na hali produkcyjnej etc
3. Gornictwo - zdrowie, ochrona i srodowisko. Zdalne kontrolowanie pojazdow, widocznosc zasobow, czy wszyscy opuscili strefe zagrozenia, zarzadzanie flota
4. Nafta i Gaz - `wydobycie,transmisja, dystrybucja - monitoring, ciaglosc pracy, optymalizacja wylaczania i wlaczania, ciglosc pracy

Systemy przemyslowe a bezpieczenstwo

Konwergencja dwoch swiatow (IT i OT)
Roznica miedzy it a ot

. W swiecie it, glownie cybersecurity, gdy w ot mamy tez ochrone produkcji, pracownikow czy procesu np. reakcje chemicznej

It - dane scentralizowane. OT - dane bardzo rozproszone
It - nowoczesne rozwiazania. OT - sprzed majacy ok 10-20 lat
It - komponenty często aktualizowane. OT - rzadkie aktualizacje i często przez zewn organizacje (zagrozenie)

Rozne ataki i zagrozenia.
IT - zlosliwe oprogramowanie, unieruchoienie uslugi, zainfekowane urzadzenia etc
OT - dodatkowo - zwykle niautoryzowne czy samowolne instrukcje wykonane dodatkowo

Kooperacja miedyz IT a OT - it zazwyczaj ma wieksza wiedze w kontekscie cybersecurity, a Ot w kontrkscie przemyslowych procesow.

Filary bezpieczenstwa

1. Inwentaryzacja zasobow (identyfikacja wszystkiego srldowiska IT/OT)
2. Architektura i segmentacja - izolacja rozprzestrzeniania się zagrozen. Architektura istotna bo ciezko zmienic potem. Potem jakas zmiana procesu - architektura musi być rozszerzalna
3. Wykrywanie zagrozen
4. IT/OT/SOC - calosciowy wglad w zachodzace zdarzenia, analiza sledzcza i procedura zapobiegania

IPS - system blokowania znanych atakow, glownie na podstawie sygnatur. Trzeba tez uwazac, żeby nie zrobic tak, ze pomimo tego ze wprowadzamy ochrone przed dana sygnatura, a to może tez zablokowac jakis element procesu. Bardziej w strefie IDMZ.

IDS - zespoly bezpieczenstwa. Mogą mieć rozne postacie:
CSIRT, SIRT, CIRT, SOC (...response team) - zespoly zwykle kilkupoziome, gdzie 1 poziom zajmuje się calodobowym wykrywaniem incydentow, a wyzsze ich weryfikacja i badaniem ich.

Podzialy na strefy i kontrola ruchu
ISA-99 / IEC-62433 Zones and Confuits
Zone - posiada jasno wyznaczone granice fizyczne i logiczne, oddzielajace elementry znajdujace się w niej od tego co na zewnatrz. Obejmuje komponenty realizujace wspolne zadania i wyamagajjace podobnego traktowania.
Conduit - kanal - polaczenia, umozliwiaja wymiane informacji miedzy strefami, dodatkowe funkcje bezpieczenstwa w tym filtrowania i inspekcji

Protokoly (będą wykorzystywane na labach)

BACnet/IP	Automatyka inteligentych budynkow	47808 UDP
DNP 3	Uzywany powszechnie w energetyce	20000TCP/UDP
EIP(EtherNet/IP)	Uzywany przeez CIP (Common Industrial protocol), krory jest popularny w automatyce rzemyslowej	44818 tcp/ 2222 UDP
ISO/TSAP	Iso Transport service access point stosowany glownie przez siemens i iccp	102 TCp
Modbus/TCP	Automatyka przemyslowa i budynkowa	502 tcp
MQTT over HTTP	Message queue Telemetry transport - M2M/Iot	1883, 80 tcp
MQTT over HTTPS	-||-	8883,443 tcp

Pare info ze swiata OT:
Urzadzenia OT zazwyczaj nie maja dostepu do neta
Umieszenie urzadzen ot w kwarantannie może spowodowac powazne szkody
Powszechne jest stosowanie niepolaczonych ze soba segmentow sieci
Sa tam niewspierane już systemy operacyjne, mogą nie mieć roznych patchy
Urzadzania i procesy dzialaja 24/7/365
Komponenty Ot stosuja typowe dla siebie protokoly komunikacji

Wyklad 2

Saturday, January 8, 2022 10:06 AM

ACL - lista kontroli dostepu
Sekwencyjna lista warunkwoa zezwolen i zakazow
Jeżeli warunek sprawdzenia pasuje, to dostaje akcje permit, lub zakazu deny a pozostale warunki nie sa sprawdzane
+ reszta, np. deny all
Najczesciej stosowane - filtrowanie ruchu

Rodzaje list kontroli dostepu do filtrowania:
Standard ACL - jedynie adres zrodlowy pakietu
Extended ACL - sprawdzaja czesc zdrodlowa i docelowa pakietu i daja mozliwosc wskazania protokolu L3./L4 i tworenia warunjkow w opartciu o jego pola

Konfiguracja:
Wszystkie reguly skladajace się na numerowana ACL maja ten san unikalny id
Standard acl <1-99> oraz <1300-1999>
Extended acl <100-199> oraz <2000-2699>

Do tworzenia warunkow stosuje się Wildcard Mask (nie musi być ciagla)

Maski blankietowej nie należy mylic z maska podsieci. Jej zapis jest kropkowo dziesietny jest odwrotnosci bitowa maski podsieci (255.255.255.255 - maska podsieci)
Maska blankietowa stosowana jest do dopasowan bitowych (zera wymuszaja dopasowanie bitowe), a jedynki nie wymuszaja dopasowania bitowego

Maska podsieci - jedynki okreslaja czesc sieci a 0 czesc hosta
Jezeliw wiec w masce blankietowej damy same 0 - tzn ze wszystkie bity musza się zgadzac
A same 1ki, tzn ze wszystko może być dowolne

Przykład chcemy filtrowac 10.0.x.10. wiec dajemy maske blankietowa 0.0.255.0 - czyli 10.0.x.10 - numery musza się zgadzac idealnie, a x jest dowolne

Skladnia standardowej ACL:
Access-list NR {permit|deny|remark| SRC-IP [WILD-MASK] [log] - zmienne NR, SRC-IP, WILD-MASK

Usuniecie ACL
No access-list NR

Weryfikacja ustawien ACL
Show access-list
Show ip access-list
Do show run | s access-list 1 (do - polecenie ze stanu wyzej)

Przykladowe zastosowanie nieciaglej maski blankietowej:
Dopasowanie tylko nieparzystyc adresow IP z 10.248.1.0/24
0001010.11111000.00000001.00000001 10.228.1.1
0000000..00000000.00000000.11111110 - 0.0.0.254

Przykladowe dopasowanie tylko parzystych adresow IP z 10.248.2.0/24
0001010.11111000.00000010.00000000 10.248.2.0
00000000.00000000.00000000.11111110 0.0.0.254

Router> - user exec
Router# privilaged exec - żeby wejsc trzeba uzyc polecenia enable
Router(config)# global connfiguration, aby wejsc uzyc polecenia configure
Router(config-if)# interface confguration
Router(config-router)# router rip

I jak chcemy korzystac z polecen np. z poziomu router# bedac w router(config)# to trzeba uzyc polecenia "do"

Skladnia acl rozszerzonego
Access-list nr {permit|deny|remark} PROTO SRC-IP WILD-MASK [OPER SRC-PORT] DST-IP WILD-MASK [OPER DST-PORT] [PROTO-FLAGS] [log]
Jest mozliwosc przenumerowanie wierszy listy ACL - rearrange (np. zmienienie dlugosci sekwencji0
<cr> oznacza ze nie trzeba wiecej parametrow

Przypisanie ACL: ip access-group ACL(nazwa) - trzeba być w configu interface'a
Weryfikacja: show ip interface INTERFACE-NAME
Do graniczenia dostepu zdalnego stosuje się listy standardowe. Przypisanie listy ACL do linii wirtualnych: Router(config-line)# access-class ACL {in|out}
Weryfikacja przypisania list aact do linii wirutalnej (pokaze tylko listy numerowane, ale nazwane dzialaja): show line

TCP.
Establised -> przepuszcza wszystkie pakiety z flagami ACK i RST(bo takie flagi sa w nawiazanych polaczeniach)

Po | można uzywac include, section, begin - np. show running-config | include nae-server - to będzie wyswietlalo running-config z podanym name-server
Section - sekcja konfiguracji
Begin - zaczyna się od zadanego wzorca
Exclude - wszystko bez linii podanej w exclude np.. Show ip interface brief | exclude unassigned

Virtual terminal - VTY - można je wlaczyc Router(config)# line vty 0 4(5 linii). Mogą slcuzyc do zdalnego logowania np.. Wszystkie linie będą mieć to samo ustawienie.

Port security - pozwala okreslic jakie adresy ac lub jaka ich ilosc może pojawic się na portcie. Mechanizm do implementacji na portach docelowych
Sposób uczenia się adresu MC:

- Dynamic (uczy się dynamicznie i zapomina po zmienie stanu portu)
- Static - statyczna konfiguracja dozwolnego/dozwolonyc adresow MAC na danym portcie
- Sticky - uczy się adresow dynamicznie, ale nie zapomina po zmianie stanu portu (dopisuje adresy do running-config)

Sposób naruszenia bezpieczenstwa:

- Przekroczenie dopuszczalnej ilosci adresow Mac na porcie
- Pojawienie się na innym portcie w ramach tego samego VLAN już nauczonego adresu MAC

Reakcja na naruszenie bezpieczenstwa: (można implementowac per interface)

- Shutdown (port jest wlaczany przez przejdsci do stanu err-disabled (DOMYSLNE))
- Restrict (odrzuca ruch oraz loguje i zlicza zdazenia (syslog, SNMP Trap, port Security Counters)
- Protect - tylko odrzuca ruch naruszajacy bezp (nie dostajemy zadnych informacji o atakach)
- Report - podobnie jak restrict, niemniej po przekroczeniu limitu bezpiecznych adresow - nie blokuje znanych mac

Podstawowa konfiguracja
Uruchomienie funkcji na porcie: switch port-security

Konfiguracja statycznego wpisu bezp adres na porcie
Switchport port-security mac-address adres-mac

Zmiana ilosci dozwolonych bezp adresow na porcie (wszystkich(czyli dynamiczn), dynamiczn + static, static albo lepkich)
Switchport port-security maximum ILOSC

Konfiguracja lepkiego uczenia się bezpiecznych adresow na porcie (dopisywanie do running-config, stad bez adresy będą usuwane po restarcie urzedzenia, jeśli nie zapiszemy konfiguracji)
Switchport port-security mac-address sticky

Wyczyszczenie nauczenie bezp adresow
Clear port-security {all|configured|dynamic|sticky} [address h.h.h | interface INTERFACE]

Port z wl funkcja port security nie może być wykorzystany jako destination port dla span(switch port anylyzer), należy do interfejsu EtherChannel oraz pracowac w trybie dynamic, który wykorzystuje protokol DTP.
Jak jest dynamic port - to można go zmienic na mode: switchport mode access

Weryfikacji portow i bezp adresow:
Wylistowanie info statycznych na temat portow na których dziala port security
Show port-security

Wylistowanie all bezp adresow;
Show port-security address

Typ bezpiecznego adresu:
- SecureDynamic - nauczony dynamicznie
- SecureConfigured
-

Konfiguracja reakcji na naruszenie bezp:
Switchport port-security violation {shutdown | restrict | protect }

Info na temat stanu i konf port securit na porcie:
Show port-security interface INTERFACE

Port status wskazuje czy mechanizm jest uzbrojony i zbezpiecza jakies adresy Mac (ma jakies adresy)

Starzenie się i wygadasanie wpisow bez adres:
DynamicSecure - domyslnie adres usuwany jest po zmianie stanu portu (up.down)

Można zdefiniowac czas po którym zostanieusuniecia:
Switchport port-security aging time MINUTES

Domyslnie - czas absolutny, liczony od zapamietania adresu. Liczyony od ostatniej aktywnosci = inactivity

SecureConfigred -domyslnie nie sa usuwane, ale można wymusic ich dzialanie na ten sam czas Aging Time
To samo co wyzej, z komenda static na koncu

Port security i obsluga kilku VLAN na porcie:
Na portach w trybie Trunk można okreslic limit dozwolonych adresow dla calego portu / per VLAN:
Swietchport port-secuity maximum [vlan]

Jeżeli port obsluguje Voice VLAN to należy ustawic limit adresow na dwa plus ilosc dozwolonych adresow w Data VLAn. Wynika to z faktu, ze adres MAC telefonu poczatkowo zostjae poznany w data VLAN a po wymianie CDP nauczony w Voice VLAn. Da się ustawic limit adresow per Voicei Data VLAN
Switchport port-security maximum N / M vlan acess / X vlan voice

Jeśli korzystamy z violation mode shutdown - warto ustawic blokowanie per vlan (domyslnie caly port):
Swithport port-secuity violation shutdown vlan

W takich przypadkach nie zaleca się konfigracji violation mode na protect - tryb ten wylacza dla kazdego portu uczenie się adresow, gdy jeden z vlan przekroczy swój limit (nawet jeśli pozostale nie)

Stan errdisabled (i przywracanie)
Przywrocenie wymaga:
-reinicjalizacji portu:
Shutdown
No shutdown

Skonfigurowania automatycznego przywracania takich portow do dzialania co okreslony czas:
Errdusabke recovery cause psecure-violation
Errdisable recovery interval 300 -- defaultowe

Weryfikacja konfiguracji:

Show errdisable recovery	`

Czesc wprowadzeniowa dla nieogrnietych w CLI Ciskowych

Saturday, January 8, 2022 12:33 PM

SSH - uruchomienie uslugi:
Router(config)# Crypto key generate rsa modulus 2048

Zmiana versji:
Ip ssh version 2

Dobra praktyka jest zdefiniowanie stalego interfaejsu z którego będzie nawiazywane polaczenie ssh:
Ip ssh source-interface Loopback0

Sposób uzycia klienta SSh w Cisco IOS
Ssh -l user5 10.248.255.1

Ustawienie username i hasla w klucz:
Username user5 secret haslo

Definiowanie hostname: hostname x
Definiowanie domain-name: ip domain-name networkers.local
..

Po wygenerowaniu ssh:
Username user5 secret haslo
Line vty 0 4

Telnet:

Tryb uprzywilejowany:
Telnet xxx
Telnet 10.248.255.1

Przez domyslny protokol transportu konsoli:
Xxx
10.248.255.1

- Wiec telnet jest domyslnym sposobem komunikacji

No ip domain lookup - wylaczenie wyszukiwania nazw w trybie exec

Jak się można dostac do urzadzenia? Albo przez fizyczny port, albo vty
Fizyk:
Line console 0
Password xxx
Login

VTY:
Line vty 0 4
Password haslo
(login jest domyslne)

Ustawienie poziomu:
Privilage 15

Żeby haslo było zakodowane z uzyciem MD5:
Enable secret haslo

Zalecany algorytm - enable algorithm-type scrypt secret HASLO

Można wlaczyc password-encryption hasla niezaszyfrowania hasel i kluczy:
Service password-encryption
No service password-encryption (to jest tylko bardzo latwy do odwrocenia alg. Sluzy glownie żeby ktos nie podejrzal przez ramie)

Tworzenie kont userow:
Username user1 password HASLO - ciulowe
Username user2 secret HASLO - ..
Username user3 algorithm-type md5 secret HASLO
Username user4 algorithm-type sha256 secret HASLO
Username user5 algorithm-type scrypt secret HASLO

Logowanie do userow:

Konifguracja linii konsoli do korzystania z bazy userow lokalnej:

Line console 0
    Login local
    Privalege level 15

VTY: line vty 0 4
    Login local

User z uprawnieniem do trybu uprz:
Username name6 privilege 15 secret HASLO

Odzyskiwanie hasla na routerze - można odzyskac typu 0-7. Wymagany fizyczny dostep
- wyl i wl urzadzenie
- Po wyswietlnie nazywy platformy należy wyslac sygnal BREAK, co spowoduje przyjscie do trybu ROMmon (
- Dokonac zmiany wartosci rejestru konf na 0x2142 - confreg 0x2142
- Przeladowac urzadzenie by wczytalo nowa wartosc: reset
- Przejscie do trybu privileged EXEC
- Kopia konfiguracji startowej na biezacej i wl interface: copy startup-config running-config
- Przywrocenie domyslnej wartosci rejestru konf: config-register 0x2142
- Zmiana hasel, wlaczenie interface'ow, zapisanie konfigow i restart

    No shutdown - podniesienie interface'a

Odzyskiwanie hasla na przelaczniku
- trzymanie jednozesnie przycisk mode przez 15s
- Flash_init
- Load_helper
- Dir flash;
- Rename flash:config.text flash:config.text.old
- Boot
- Copy flash;config.text.old running-config