An overview of ICS vulnerabilities, threats, and security measures

Based on three real-world power plants security concerns

Silvio Ranise

Relatore

Riccardo Gennaro

Studente

UNIVERSITÀ DI TRENTO

Corso di Laurea in Informatica

Trento, 2 dicembre 2022

Indice

Introduzione

L'evoluzione dell'architettura degli **Industrial Control Systems** (ICS) avvenuta negli ultimi cinquant'anni, non è andata di pari passo con lo sviluppo della loro sicurezza.

Questo ha permesso ad attori come **stati-nazioni e gruppi terroristici** di creare danni irreparabili sia ad infrastrutture che a persone.

La necessità di approcci preventivi sia attivi che passivi si fa sempre più evidente.

Introduzione

L'evoluzione dell'architettura degli **Industrial Control Systems** (ICS) avvenuta negli ultimi cinquant'anni, non è andata di pari passo con lo sviluppo della loro sicurezza.

Questo ha permesso ad attori come **stati-nazioni e gruppi terroristici** di creare danni irreparabili sia ad infrastrutture che a persone.

La necessità di approcci preventivi sia attivi che passivi si fa sempre più evidente.

Introduzione

L'evoluzione dell'architettura degli **Industrial Control Systems** (ICS) avvenuta negli ultimi cinquant'anni, non è andata di pari passo con lo sviluppo della loro sicurezza.

Questo ha permesso ad attori come **stati-nazioni e gruppi terroristici** di creare danni irreparabili sia ad infrastrutture che a persone.

La necessità di approcci preventivi sia attivi che passivi si fa sempre più evidente.

Introduzione

Area IT (Informazionale)

- Comunicazione e scambio di informazioni
- Soluzioni di sicurezza consolidate
- Buon livello di manutenzione e patching

Area OT (Operazionale)

- Controllo di apparecchiatura industriale
- Mancanza di soluzioni standardizzate
- Difficoltà in mantenimento e aggiornamento

Introduzione

Area IT (Informazionale)

- Comunicazione e scambio di informazioni
- Soluzioni di sicurezza consolidate
- Buon livello di manutenzione e patching

Area OT (Operazionale)

- Controllo di apparecchiatura industriale
- Mancanza di soluzioni standardizzate
- Difficoltà in mantenimento e aggiornamento

Introduzione

Area IT (Informazionale)

- Comunicazione e scambio di informazioni
- Soluzioni di sicurezza consolidate
- Buon livello di manutenzione e patching

Area OT (Operazionale)

- Controllo di apparecchiatura industriale
- Mancanza di soluzioni standardizzate
- Difficoltà in mantenimento e aggiornamento

Problem statement

Trends

Negli ultimi anni si rilevano i seguenti trend relativi ai sistemi trattati

- Necessità di aumento nell'**efficienza** dei processi produttivi
- Aumento della **criminalità** cibernetica
- Introduzione e revisione di **framework e standard**

Problema

Soprattutto a causa della necessità di controllo e monitoraggio remoto, gli ICS risultano non essere più *air-gapped*, esponendo i loro sistemi a reti non sicure.

Problem statement

Trends

Negli ultimi anni si rilevano i seguenti trend relativi ai sistemi trattati

- Necessità di aumento nell'**efficienza** dei processi produttivi
- Aumento della **criminalità** cibernetica
- Introduzione e revisione di **framework e standard**

Problema

Soprattutto a causa della necessità di controllo e monitoraggio remoto, gli ICS risultano non essere più *air-gapped*, esponendo i loro sistemi a reti non sicure.

Problem statement

Trends

Negli ultimi anni si rilevano i seguenti trend relativi ai sistemi trattati

- Necessità di aumento nell'**efficienza** dei processi produttivi
- Aumento della **criminalità** cibernetica
- Introduzione e revisione di **framework e standard**

Problema

Soprattutto a causa della necessità di controllo e monitoraggio remoto, gli ICS risultano non essere più *air-gapped*, esponendo i loro sistemi a reti non sicure.

Problem statement

Trends

Negli ultimi anni si rilevano i seguenti trend relativi ai sistemi trattati

- Necessità di aumento nell'**efficienza** dei processi produttivi
- Aumento della **criminalità** cibernetica
- Introduzione e revisione di **framework e standard**

Problema

Soprattutto a causa della necessità di controllo e monitoraggio remoto, gli ICS risultano non essere più *air-gapped*, esponendo i loro sistemi a reti non sicure.

Problem statement

Trends

Negli ultimi anni si rilevano i seguenti trend relativi ai sistemi trattati

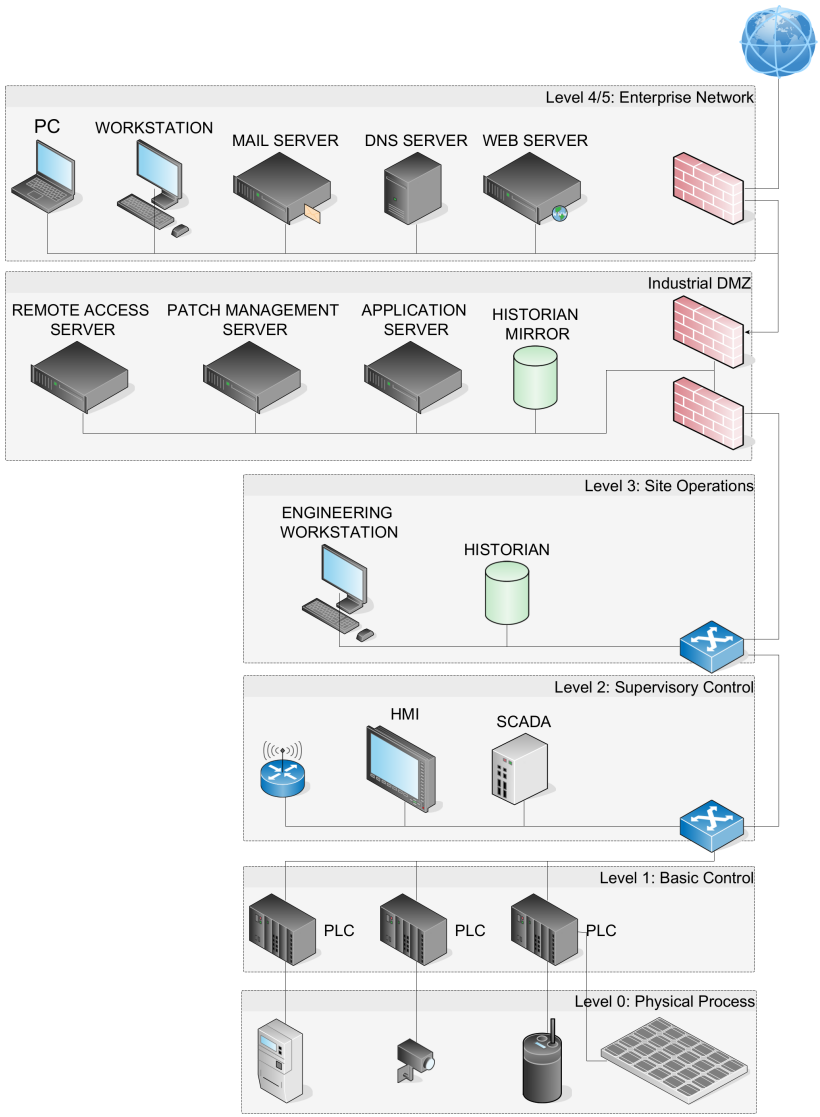
- Necessità di aumento nell'**efficienza** dei processi produttivi
- Aumento della **criminalità** cibernetica
- Introduzione e revisione di **framework e standard**

Problema

Soprattutto a causa della necessità di controllo e monitoraggio remoto, gli ICS risultano non essere più *air-gapped*, esponendo i loro sistemi a reti non sicure.

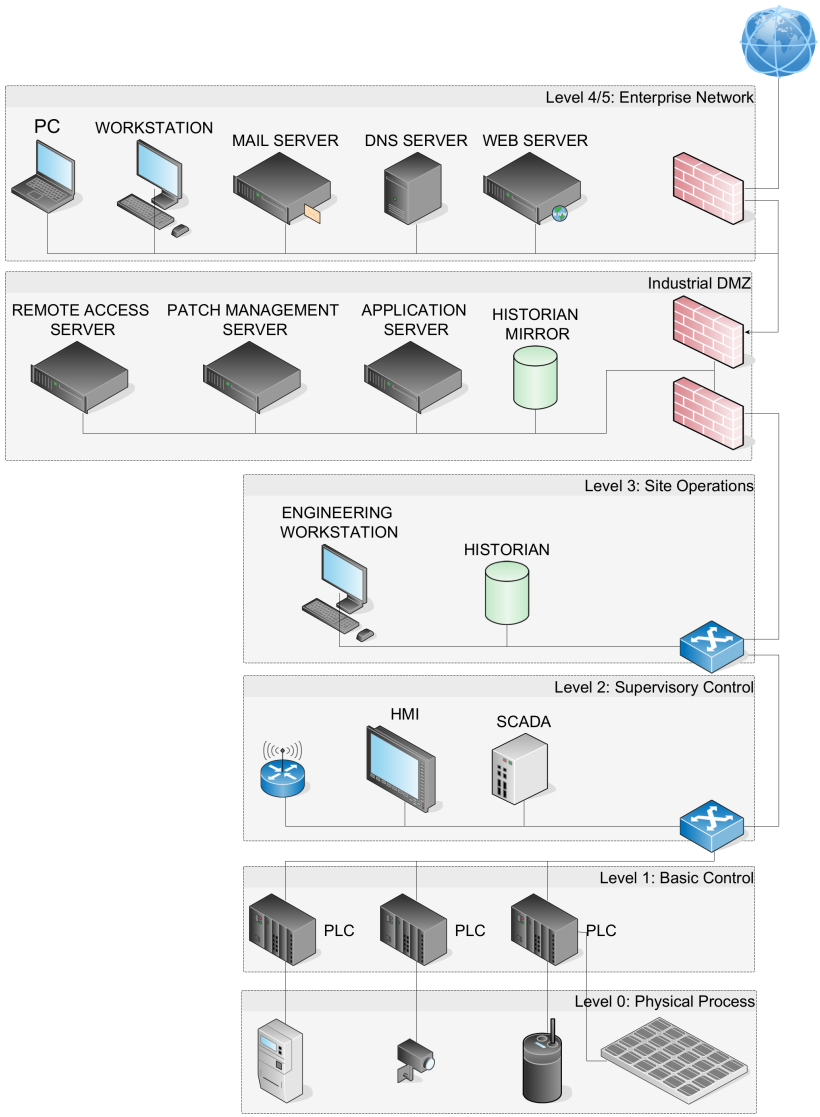
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



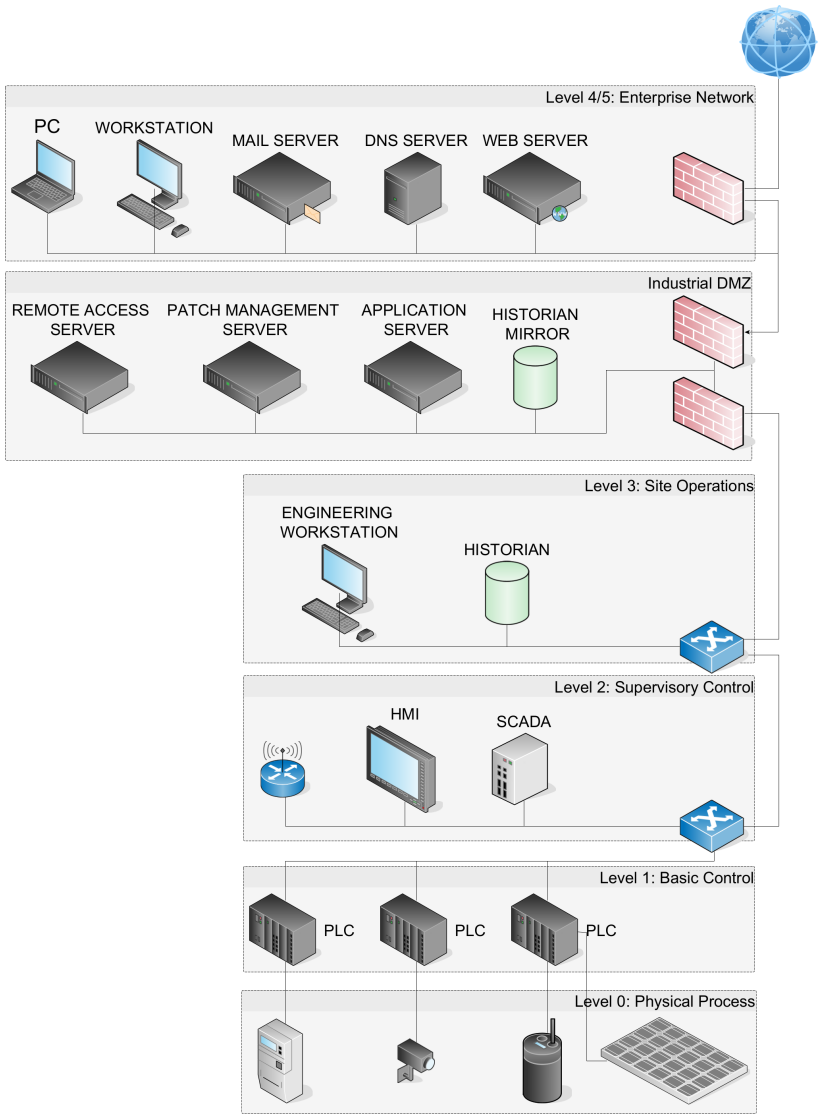
Purdue Model

- **Lvl 5**: Enterprise Network
- Lvl 4: Business planning
- DMZ
- Lvl 3: Site Operations
- Lvl 2: Supervisory Control
- Lvl 1: Basic Control
- Lvl 0: Physical Process



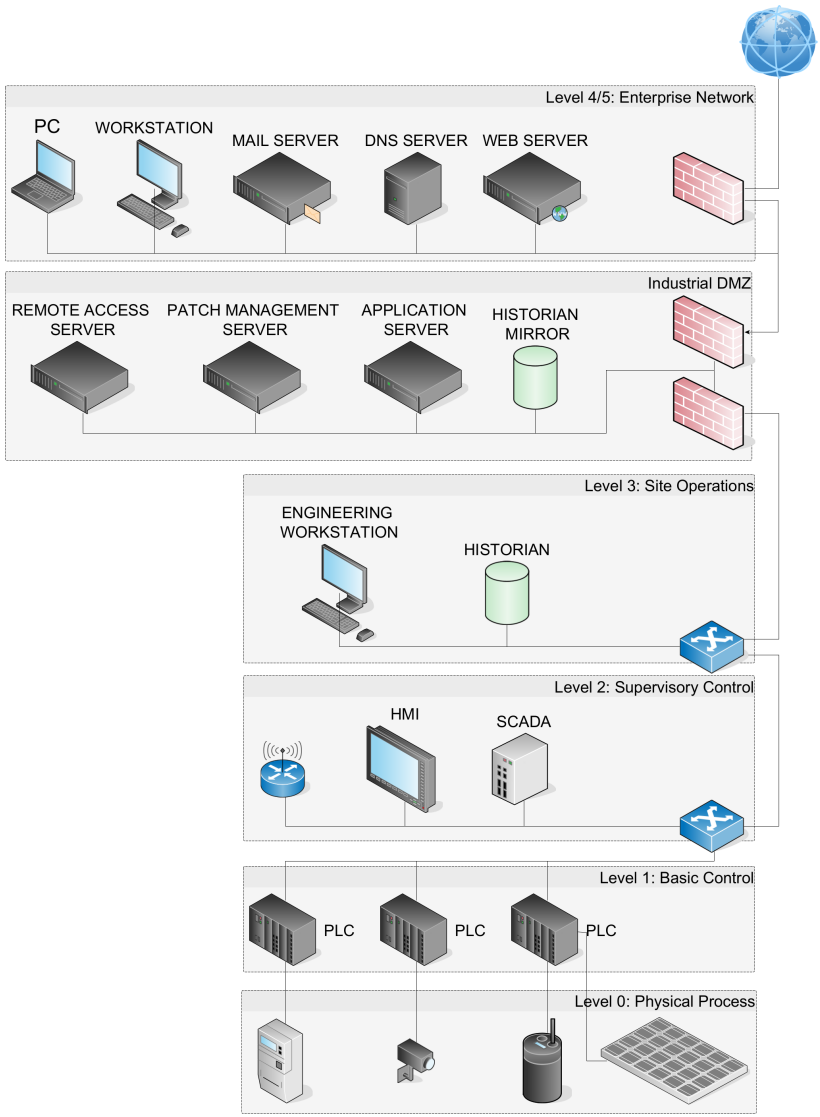
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- DMZ
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



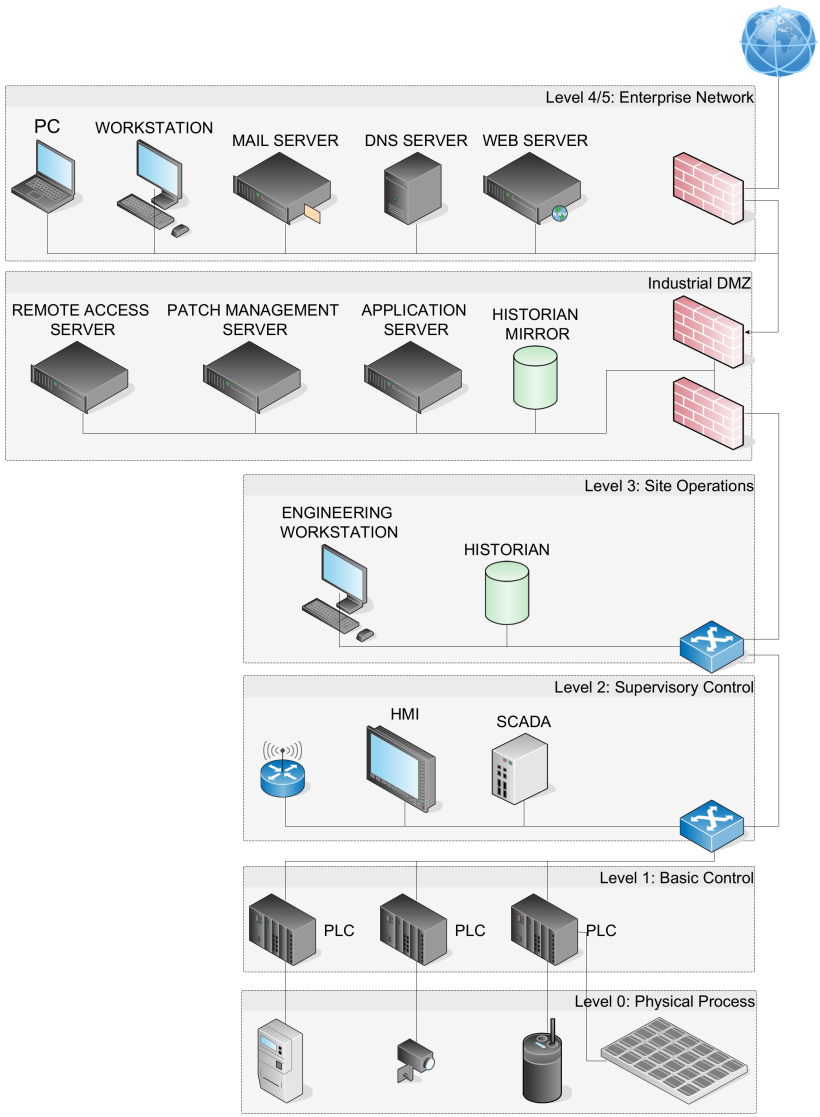
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



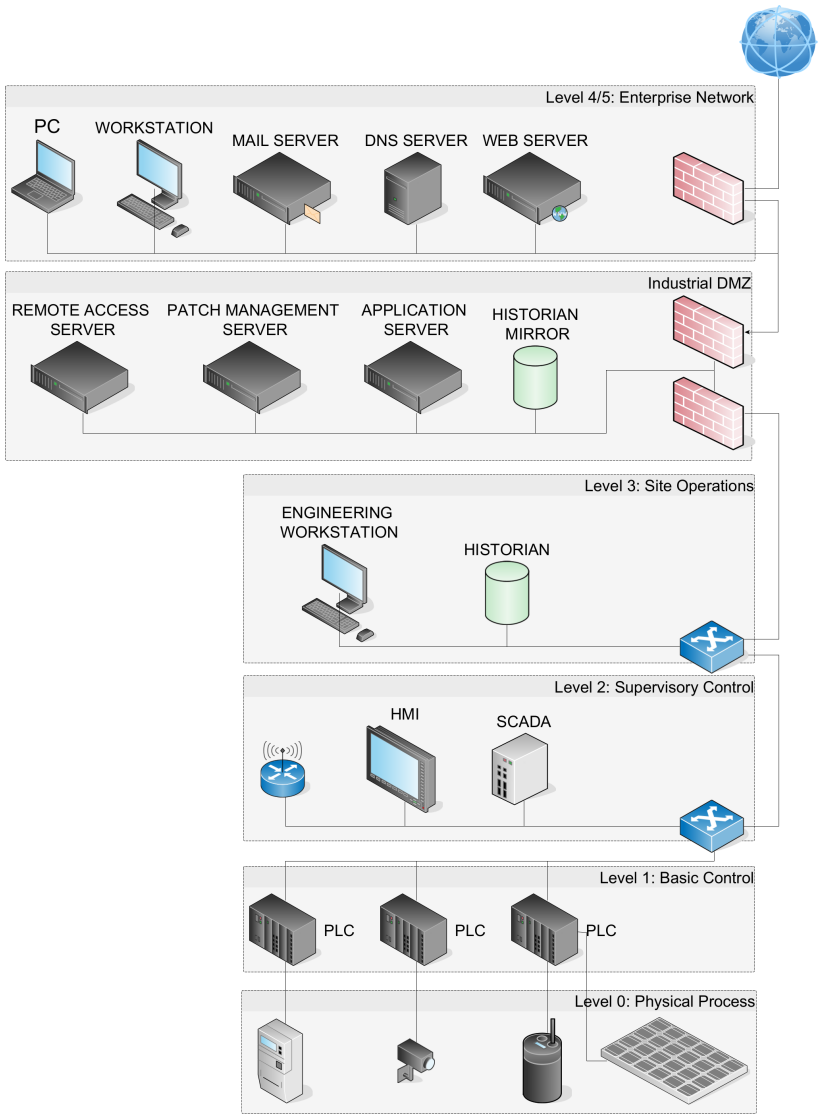
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



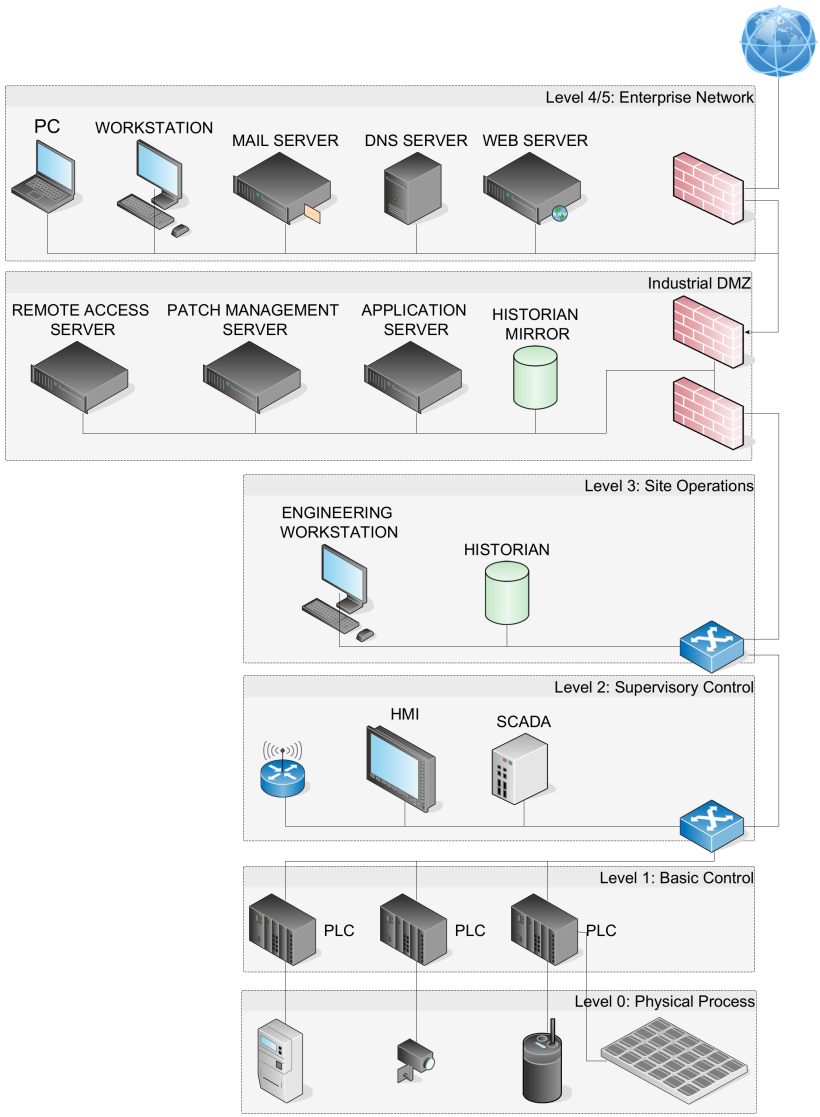
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



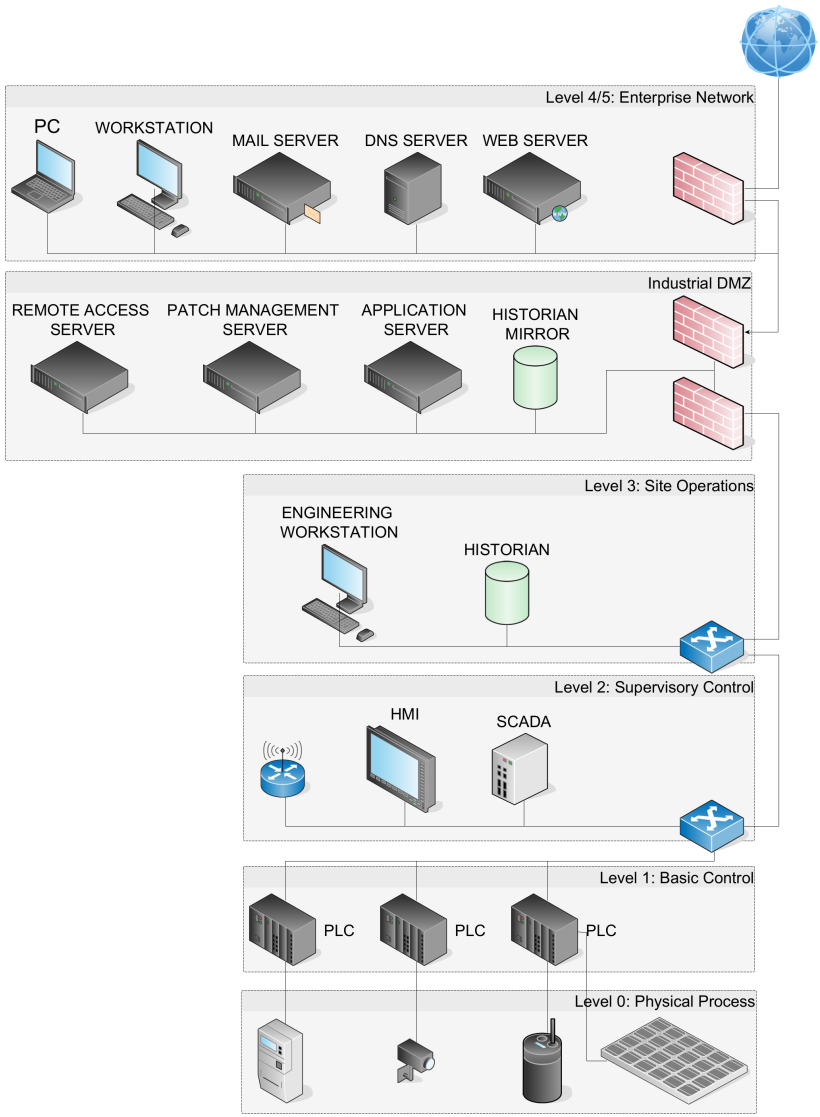
Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



Purdue Model

- **Lvl 5**: Enterprise Network
- **Lvl 4**: Business planning
- **DMZ**
- **Lvl 3**: Site Operations
- **Lvl 2**: Supervisory Control
- **Lvl 1**: Basic Control
- **Lvl 0**: Physical Process



Attack Vectors

Attack on hardware

Nel momento in cui l'attaccante ha accesso ad un *field device*, questi può manipolare i valori delle variabili generate e lette da questo device.

Attack on software

Tecniche comuni sono *False Data Injection Attack* (FDIA), tramite SQL-Injection contro gli *historian*, oppure privilege escalation e buffer overflow sui *field device*.

Attack on communication

Molti protocolli scrivono in chiaro. Spesso non è necessario compromettere un set di dispositivi, ma risulta sufficiente interferire con la loro comunicazione.

Attack Vectors

Attack on hardware

Nel momento in cui l'attaccante ha accesso ad un *field device*, questi può manipolare i valori delle variabili generate e lette da questo device.

Attack on software

Tecniche comuni sono *False Data Injection Attack* (FDIA), tramite SQL-Injection contro gli *historian*, oppure privilege escalation e buffer overflow sui *field device*.

Attack on communication

Molti protocolli scrivono in chiaro. Spesso non è necessario compromettere un set di dispositivi, ma risulta sufficiente interferire con la loro comunicazione.

Attack Vectors

Attack on hardware

Nel momento in cui l'attaccante ha accesso ad un *field device*, questi può manipolare i valori delle variabili generate e lette da questo device.

Attack on software

Tecniche comuni sono *False Data Injection Attack* (FDIA), tramite SQL-Injection contro gli *historian*, oppure privilege escalation e buffer overflow sui *field device*.

Attack on communication

Molti protocolli scrivono in chiaro. Spesso non è necessario compromettere un set di dispositivi, ma risulta sufficiente interferire con la loro comunicazione.

Indice

Metodologia

Problem statement

Dato un subset di una rete di automazione con bassa visibilità sull'asset, si vuole

- Operare un asset inventory
- Analizzare le vulnerabilità dell'asset scoperto
- Proporre mitigazioni

Problem statement

Tutte le operazioni effettuate non possono interrompere o interferire con il processo fisico. Le mitigazioni proposte devono tenere conto della bassa compatibilità dei software SCADA.

Metodologia

Problem statement

Dato un subset di una rete di automazione con bassa visibilità sull'asset, si vuole

- Operare un asset inventory
- Analizzare le vulnerabilità dell'asset scoperto
- Proporre mitigazioni

Problem statement

Tutte le operazioni effettuate non possono interrompere o interferire con il processo fisico. Le mitigazioni proposte devono tenere conto della bassa compatibilità dei software SCADA.

Metodologia

Problem statement

Dato un subset di una rete di automazione con bassa visibilità sull'asset, si vuole

- Operare un asset inventory
- Analizzare le vulnerabilità dell'asset scoperto
- Proporre mitigazioni

Problem statement

Tutte le operazioni effettuate non possono interrompere o interferire con il processo fisico. Le mitigazioni proposte devono tenere conto della bassa compatibilità dei software SCADA.

Metodologia

Problem statement

Dato un subset di una rete di automazione con bassa visibilità sull'asset, si vuole

- Operare un asset inventory
- Analizzare le vulnerabilità dell'asset scoperto
- Proporre mitigazioni

Problem statement

Tutte le operazioni effettuate non possono interrompere o interferire con il processo fisico. Le mitigazioni proposte devono tenere conto della bassa compatibilità dei software SCADA.

Metodologia

Problem statement

Dato un subset di una rete di automazione con bassa visibilità sull'asset, si vuole

- Operare un asset inventory
- Analizzare le vulnerabilità dell'asset scoperto
- Proporre mitigazioni

Problem statement

Tutte le operazioni effettuate non possono interrompere o interferire con il processo fisico. Le mitigazioni proposte devono tenere conto della bassa compatibilità dei software SCADA.

Raccolta dati

ID	Name	Type	OS/Firmware	IP	MAC
103b724d-d79d-453e-89d5	HMI-A102	computer	Windows XP SP3	172.16.40.0	09:00:09:00:01:12
089f901d-cb58-4055-9652	ACMEincHQ_SW1	switch	Firmware: h.10.38	192.168.0.0	00:16:b9:49:b6:40
e393a902-68fb-4567-b2d1	Modicon M340 BMX P34 20	PLC	Firmware: v2.9	172.16.1.0	00:60:78:00:69:f8

Table: Esempio di asset table

Raccolta dati

Attraverso uno scan passivo si raccolgono i dati sull'asset, che comprendono

- **asset properties**, ossia IP, MAC, CPE code / Firmware version, tipo di device mappato sul Purdue model, ove possibile.
- **communication properties**, ossia protocolli usati, traffico di rete, IP di sender e receiver.

Tables separate per traffico e asset properties sono prodotte.

Raccolta dati

ID	Name	Type	OS/Firmware	IP	MAC
103b724d-d79d-453e-89d5	HMI-A102	computer	Windows XP SP3	172.16.40.0	09:00:09:00:01:12
089f901d-cb58-4055-9652	ACMEincHQ_SW1	switch	Firmware: h.10.38	192.168.0.0	00:16:b9:49:b6:40
e393a902-68fb-4567-b2d1	Modicon M340 BMX P34 20	PLC	Firmware: v2.9	172.16.1.0	00:60:78:00:69:f8

Table: Esempio di asset table

Raccolta dati

Attraverso uno scan passivo si raccolgono i dati sull'asset, che comprendono

- **asset properties**, ossia IP, MAC, CPE code / Firmware version, tipo di device mappato sul Purdue model, ove possibile.
- **communication properties**, ossia protocolli usati, traffico di rete, IP di sender e receiver.

Tables separate per traffico e asset properties sono prodotte.

Raccolta dati

ID	Name	Type	OS/Firmware	IP	MAC
103b724d-d79d-453e-89d5	HMI-A102	computer	Windows XP SP3	172.16.40.0	09:00:09:00:01:12
089f901d-cb58-4055-9652	ACMEincHQ_SW1	switch	Firmware: h.10.38	192.168.0.0	00:16:b9:49:b6:40
e393a902-68fb-4567-b2d1	Modicon M340 BMX P34 20	PLC	Firmware: v2.9	172.16.1.0	00:60:78:00:69:f8

Table: Esempio di asset table

Raccolta dati

Attraverso uno scan passivo si raccolgono i dati sull'asset, che comprendono

- **asset properties**, ossia IP, MAC, CPE code / Firmware version, tipo di device mappato sul Purdue model, ove possibile.
- **communication properties**, ossia protocolli usati, traffico di rete, IP di sender e receiver.

Tables separate per traffico e asset properties sono prodotte.

Raccolta dati

ID	Name	Type	OS/Firmware	IP	MAC
103b724d-d79d-453e-89d5	HMI-A102	computer	Windows XP SP3	172.16.40.0	09:00:09:00:01:12
089f901d-cb58-4055-9652	ACMEincHQ_SW1	switch	Firmware: h.10.38	192.168.0.0	00:16:b9:49:b6:40
e393a902-68fb-4567-b2d1	Modicon M340 BMX P34 20	PLC	Firmware: v2.9	172.16.1.0	00:60:78:00:69:f8

Table: Esempio di asset table

Raccolta dati

Attraverso uno scan passivo si raccolgono i dati sull'asset, che comprendono

- **asset properties**, ossia IP, MAC, CPE code / Firmware version, tipo di device mappato sul Purdue model, ove possibile.
- **communication properties**, ossia protocolli usati, traffico di rete, IP di sender e receiver.

Tables separate per traffico e asset properties sono prodotte.

Analisi delle vulnerabilità

ID	asset_id	cve_code	matching_cpes	cve_summary	cve_score
4f[...]c1	103b724d-[...]-89d5	CVE-2000-1218	cpe:/o:microsoft:windows_xp:-:sp3:-	The default configuration [...]	7.5
62[...]3b	089f901d-[...]-9652	CVE-2013-6926	cpe:/o:siemens:ruggedcom_system:-:-:-	The integrated HTTPS server [...]	8

Table: Esempio di table di vulnerabilità

Analisi delle vulnerabilità

A partire dai dati raccolti nella prima parte vengono prodotte analisi su

- **asset**, analizzando le vulnerabilità usando CVSS 2.0 e individuando i sistemi più vulnerabili. Una table con le CVE riscontrate è prodotta
- **architettura di rete**, dove possibile, analizzando i protocolli usati, livello di network hardening, ed eventuali violazioni di standard

Analisi delle vulnerabilità

ID	asset_id	cve_code	matching_cpes	cve_summary	cve_score
4f[...]c1	103b724d-[...]-89d5	CVE-2000-1218	cpe:/o:microsoft:windows_xp:-:sp3:-	The default configuration [...]	7.5
62[...]3b	089f901d-[...]-9652	CVE-2013-6926	cpe:/o:siemens:ruggedcom_system:-:-:-	The integrated HTTPS server [...]	8

Table: Esempio di table di vulnerabilità

Analisi delle vulnerabilità

A partire dai dati raccolti nella prima parte vengono prodotte analisi su

- **asset**, analizzando le vulnerabilità usando CVSS 2.0 e individuando i sistemi più vulnerabili. Una table con le CVE riscontrate è prodotta
- **architettura di rete**, dove possibile, analizzando i protocolli usati, livello di network hardening, ed eventuali violazioni di standard

Analisi delle vulnerabilità

ID	asset_id	cve_code	matching_cpes	cve_summary	cve_score
4f[...]c1	103b724d-[...]-89d5	CVE-2000-1218	cpe:/o:microsoft:windows_xp:-:sp3:-	The default configuration [...]	7.5
62[...]3b	089f901d-[...]-9652	CVE-2013-6926	cpe:/o:siemens:ruggedcom_system:-:-:-	The integrated HTTPS server [...]	8

Table: Esempio di table di vulnerabilità

Analisi delle vulnerabilità

A partire dai dati raccolti nella prima parte vengono prodotte analisi su

- **asset**, analizzando le vulnerabilità usando CVSS 2.0 e individuando i sistemi più vulnerabili. Una table con le CVE riscontrate è prodotta
- **architettura di rete**, dove possibile, analizzando i protocolli usati, livello di network hardening, ed eventuali violazioni di standard

Proposte di mitigazione

ID	alert_type	time	description	risk	protocol	ip_src	ip_dst
84[...]b7	SIGN:MALWARE-DETECTED	**2022-03-25** 12:12:27.120	Suspicious transferring [...]	10	smb	192.168.2.0	192.168.1.0
84[...]d4	SIGN:ACCESS-DENIED	**2022-03-27** 14:34:23.97	Unsuccessful login [...]	8.5	smb	192.168.2.0	192.168.1.0
54[...]c5	SIGN:SYN-FLOOD	**2022-03-27** 15:32:21.105	A suspicious [...]	7	tcp	192.168.1.0	192.168.0.0

Table: Esempio di table di allerte

A partire dall'analisi delle vulnerabilità, delle proposte e osservazioni su come migliorare la sicurezza della rete sono effettuate.

Inoltre, la rete è sottoposta a monitoraggio continuo tramite un IDS/SIEM per raccogliere le allerte causate da deviazioni dalla baseline delle comunicazioni.

Proposte di mitigazione

ID	alert_type	time	description	risk	protocol	ip_src	ip_dst
84[...]b7	SIGN:MALWARE-DETECTED	**2022-03-25** 12:12:27.120	Suspicious transferring [...]	10	smb	192.168.2.0	192.168.1.0
84[...]d4	SIGN:ACCESS-DENIED	**2022-03-27** 14:34:23.97	Unsuccessful login [...]	8.5	smb	192.168.2.0	192.168.1.0
54[...]c5	SIGN:SYN-FLOOD	**2022-03-27** 15:32:21.105	A suspicious [...]	7	tcp	192.168.1.0	192.168.0.0

Table: Esempio di table di allerte

A partire dall'analisi delle vulnerabilità, delle proposte e osservazioni su come migliorare la sicurezza della rete sono effettuate.

Inoltre, la rete è sottoposta a monitoraggio continuo tramite un IDS/SIEM per raccogliere le allerte causate da deviazioni dalla baseline delle comunicazioni.

Indice

Progetto

- **Atos SpA - Milano**
  Multinazionale francese area servizi IT e consulenza.
- Valutazione e miglioramento della security posture di centrali elettriche di terze parti.
- Marzo 2022 - Aprile 2022

Progetto

- **Atos SpA - Milano**
  Multinazionale francese area servizi IT e consulenza.
- Valutazione e miglioramento della security posture di centrali elettriche di terze parti.
- Marzo 2022 - Aprile 2022

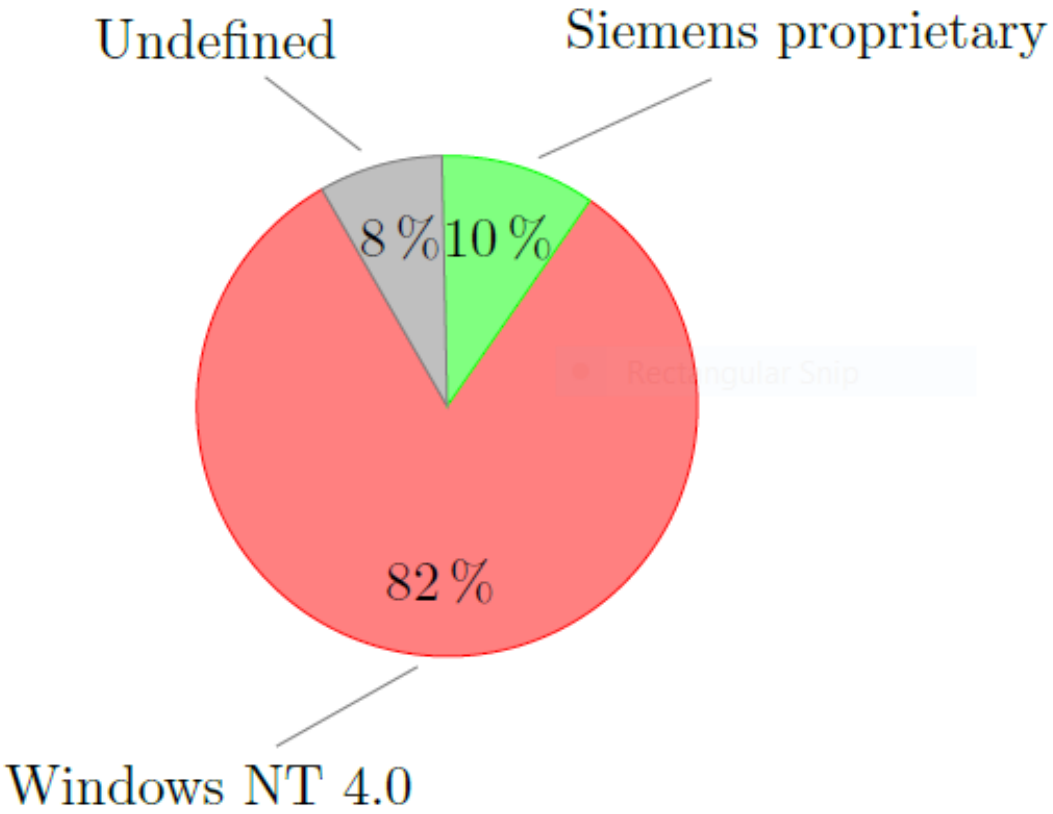
Progetto

- **Atos SpA - Milano**
  Multinazionale francese area servizi IT e consulenza.
- Valutazione e miglioramento della security posture di centrali elettriche di terze parti.
- Marzo 2022 - Aprile 2022

Progetto

- **Atos SpA - Milano**
  Multinazionale francese area servizi IT e consulenza.
- Valutazione e miglioramento della security posture di centrali elettriche di terze parti.
- Marzo 2022 - Aprile 2022

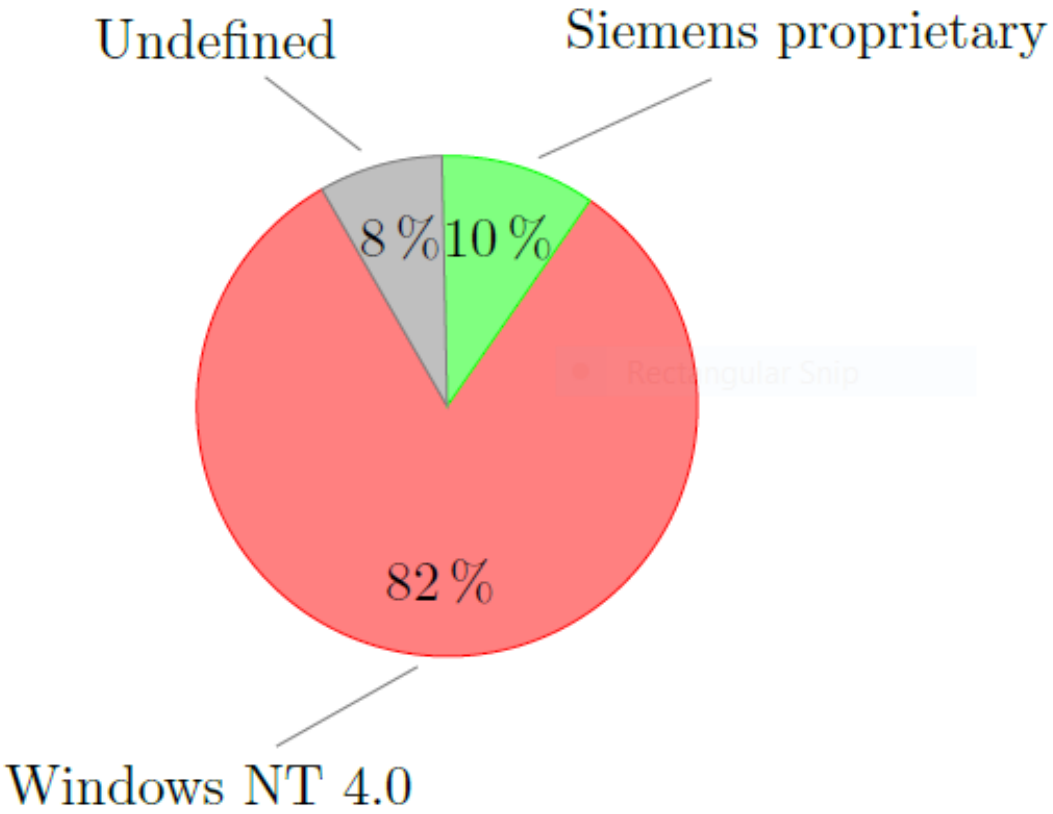
Sistemi livello 1



Basic control implementato via sistemi Windows NT 4

- Sitemi obsoleti
- Non specific-purpose

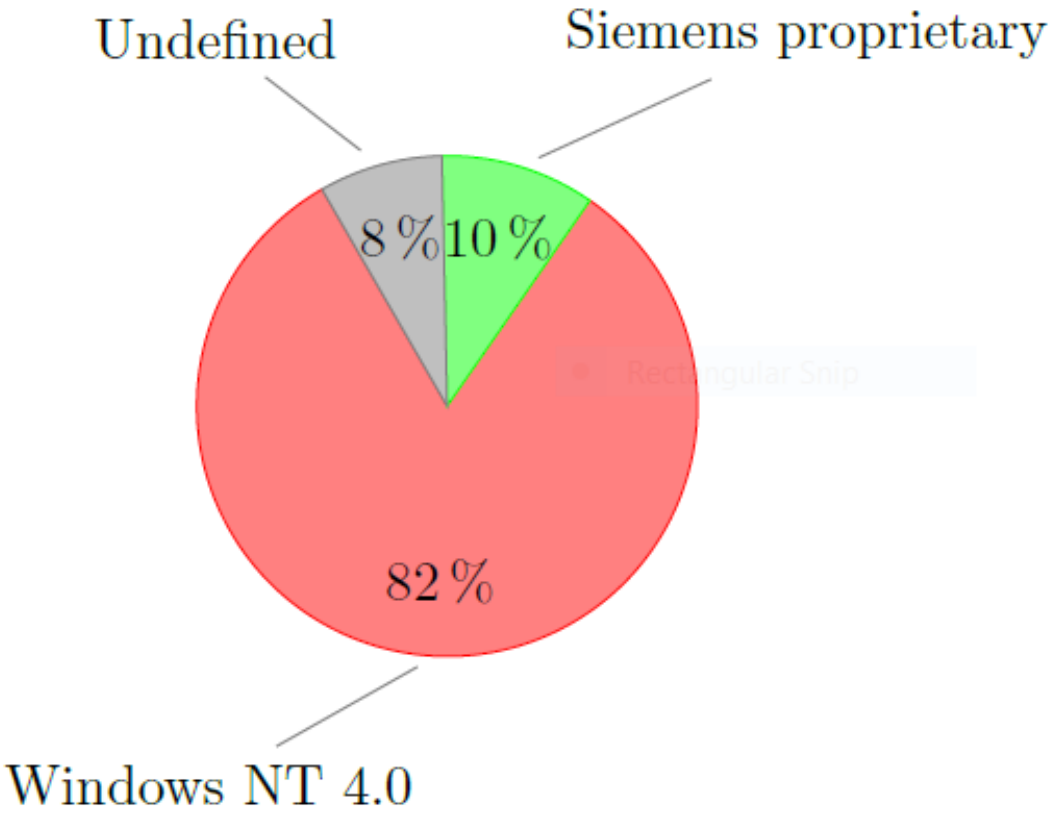
Sistemi livello 1



Basic control implementato via sistemi Windows NT 4

- Sitemi obsoleti
- Non specific-purpose

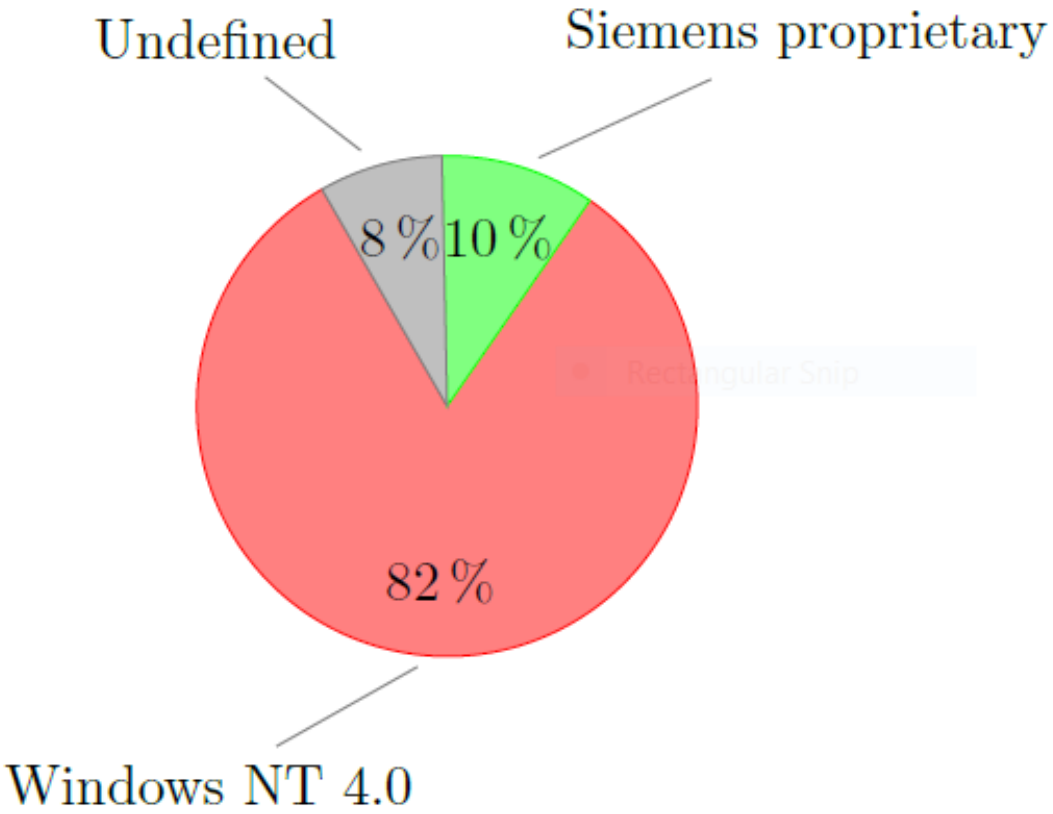
Sistemi livello 1



Basic control implementato via sistemi Windows NT 4

- Sitemi obsoleti
- Non specific-purpose

Sistemi livello 1



Basic control implementato via sistemi Windows NT 4

- Sitemi obsoleti
- Non specific-purpose

Sistemi livello 2 e 3

CPE	*IP Count*
Windows 2003	4
Windows Server 2003 SP2	2
Windows Server 2003 R2 SP2	1
Windows 7	1
Windows 2000	25
Windows XP SP2	24
Windows XP SP3	7
Not mapped	24

Site Operations e *Supervisory Control* gestiti da sistemi EOL, spesso non aggiornati alla loro ultima versione.

Sistemi livello 2 e 3

CPE	*IP Count*
Windows 2003	4
Windows Server 2003 SP2	2
Windows Server 2003 R2 SP2	1
Windows 7	1
Windows 2000	25
Windows XP SP2	24
Windows XP SP3	7
Not mapped	24

Site Operations e *Supervisory Control* gestiti da sistemi EOL, spesso non aggiornati alla loro ultima versione.

Protocolli

Lo scambio di variabili per la gestione del processo avviene tramite `SMB` (Samba).

Protocol	*Link Count*
netbios-ns	661
smb	286
browser	207
netbios-ssn	80
dce-rpc	55
lldp	40
opc	33
igmp	16
ssdp	11
telnet	6
modbus	3
others	57
Not mapped	333

Assessment

Architettura del network

- Due router sono esposti all'Internet. Protezione VPN-based
- Violazione `RFC 1918` (separazione IP pubblici e privati)
- Impropria segmentazione tra `VLAN 172.31.0.0/24` e `192.168.2.0/24`

Assessment

Architettura del network

- Due router sono esposti all'Internet. Protezione VPN-based
- Violazione `RFC 1918` (separazione IP pubblici e privati)
- Impropria segmentazione tra `VLAN 172.31.0.0/24` e `192.168.2.0/24`

Assessment

Architettura del network

- Due router sono esposti all'Internet. Protezione VPN-based
- Violazione `RFC 1918` (separazione IP pubblici e privati)
- Impropria segmentazione tra `VLAN 172.31.0.0/24` e `192.168.2.0/24`

Assessment

Architettura del network

- Due router sono esposti all'Internet. Protezione VPN-based
- Violazione `RFC 1918` (separazione IP pubblici e privati)
- Impropria segmentazione tra `VLAN 172.31.0.0/24` e `192.168.2.0/24`

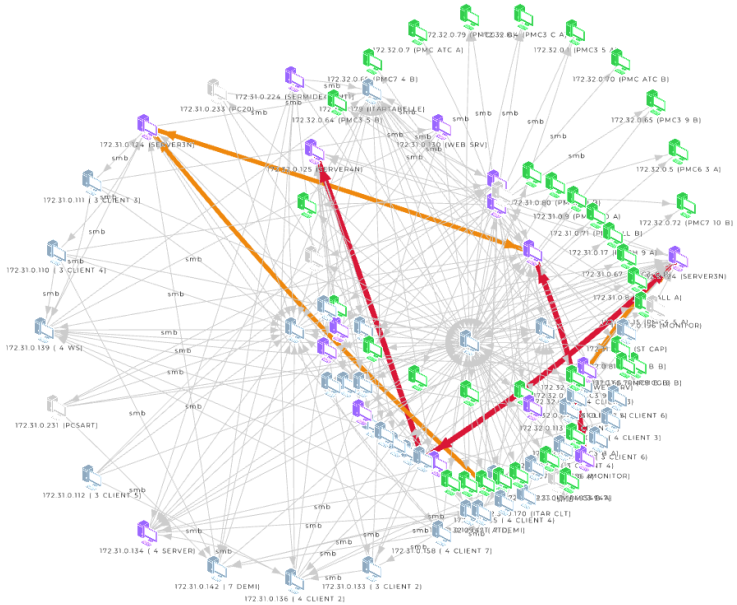
Assessment

Architettura del network

- Due router sono esposti all'Internet. Protezione VPN-based
- Violazione `RFC 1918` (separazione IP pubblici e privati)
- Impropria segmentazione tra `VLAN 172.31.0.0/24` e `192.168.2.0/24`

Common Weakness Enumeration	*Percentage*	*Most recurring CVE*	CVSS2
CWE-20: Improper Input Validation	18.9	CVE-2005-0050	10.0
CWE-119: Buffer Overflow	18.8	CVE-2005-1987	7.5
CWE-264: Broken Access Control	13.3	CVE-2010-0232	7.2
CWE-399: Resource Management Errors	12.2	CVE-2010-0269	10.0
CWE-94: Code Injection	9.9	CVE-2008-4835	10.0
CWE-362: Race Condition	6.1	CVE-2010-0021	7.1
CWE-189: Numeric Errors	5.2	CVE-2009-2511	7.5
CWE-200: Information Exposure	3.8	CVE-2009-0086	10.0
CWE-16: Configuration	1.7	CVE-2008-4609	7.1

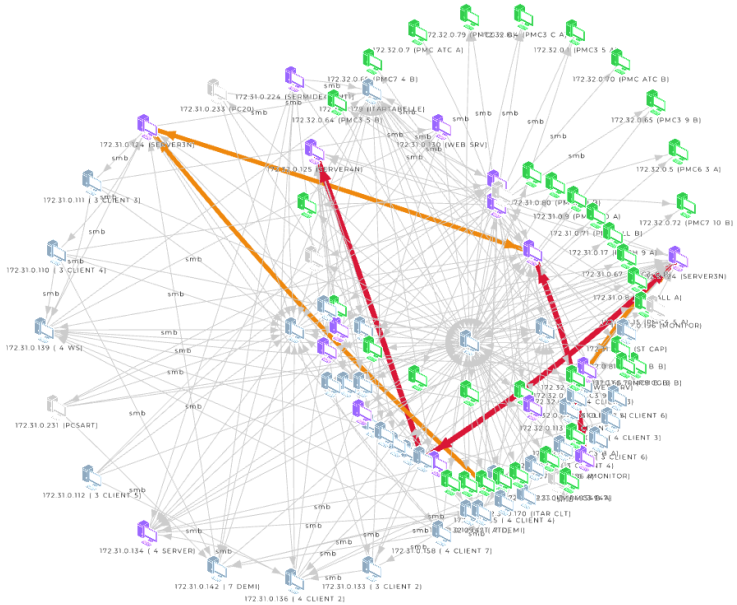
Allerte IDS



Allerte da ottobre 2021

- Multipli `OPC` network scan
- Multipli `Profinet` network scan
- Richieste di accesso negate a share `MS SMB` ad alta frequenza
- Richieste multiple di apertura di share `MS SMB` anonime

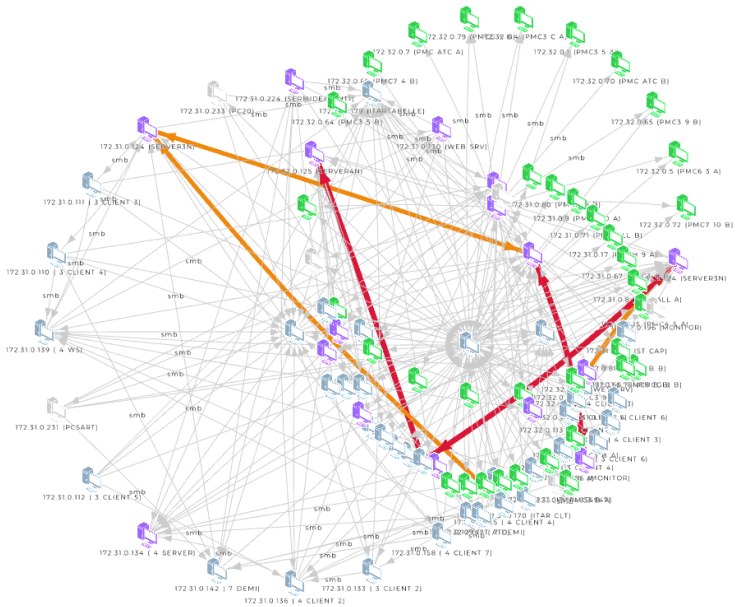
Allerte IDS



Allerte da ottobre 2021

- Multipli `OPC` network scan
- Multipli `Profinet` network scan
- Richieste di accesso negate a share `MS SMB` ad alta frequenza
- Richieste multiple di apertura di share `MS SMB` anonime

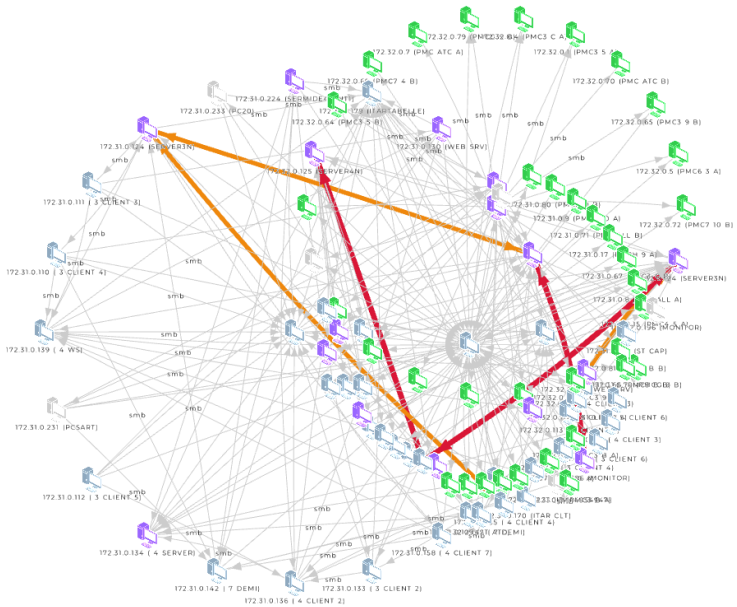
Allerte IDS



Allerte da ottobre 2021

- Multipli `OPC` network scan
- Multipli `Profinet` network scan
- Richieste di accesso negate a share `MS SMB` ad alta frequenza
- Richieste multiple di apertura di share `MS SMB` anonime

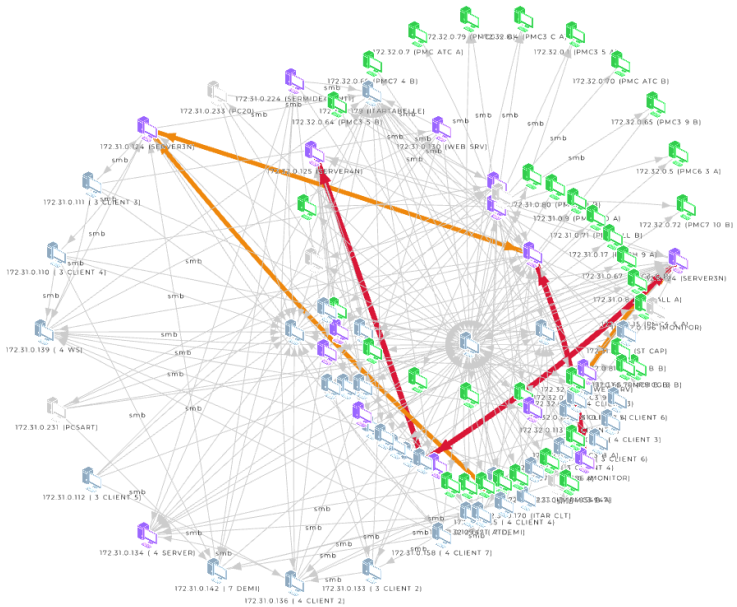
Allerte IDS



Allerte da ottobre 2021

- Multipli `OPC` network scan
- Multipli `Profinet` network scan
- Richieste di accesso negate a share `MS SMB` ad alta frequenza
- Richieste multiple di apertura di share `MS SMB` anonime

Allerte IDS



Allerte da ottobre 2021

- Multipli `OPC` network scan
- Multipli `Profinet` network scan
- Richieste di accesso negate a share `MS SMB` ad alta frequenza
- Richieste multiple di apertura di share `MS SMB` anonime

Mitigazioni

Proposte

- Firewall setup sul perimetro esposto di `VLAN 10.0.28.0/24` e `VLAN 192.168.2.0/24`
- Revisione della politica di segmentazione, come in paradigma *"zones and conduits"* di `IEC 62443`
- Correggere la violazione dell'uso di IP pubblici come privati
- Mantenere offline le workstation (EWS) quando non necessarie

Mitigazioni

Proposte

- Firewall setup sul perimetro esposto di `VLAN 10.0.28.0/24` e `VLAN 192.168.2.0/24`
- Revisione della politica di segmentazione, come in paradigma *"zones and conduits"* di `IEC 62443`
- Correggere la violazione dell'uso di IP pubblici come privati
- Mantenere offline le workstation (EWS) quando non necessarie

Mitigazioni

Proposte

- Firewall setup sul perimetro esposto di `VLAN 10.0.28.0/24` e `VLAN 192.168.2.0/24`
- Revisione della politica di segmentazione, come in paradigma *"zones and conduits"* di `IEC 62443`
- Correggere la violazione dell'uso di IP pubblici come privati
- Mantenere offline le workstation (EWS) quando non necessarie

Mitigazioni

Proposte

- Firewall setup sul perimetro esposto di `VLAN 10.0.28.0/24` e `VLAN 192.168.2.0/24`
- Revisione della politica di segmentazione, come in paradigma *"zones and conduits"* di `IEC 62443`
- Correggere la violazione dell'uso di IP pubblici come privati
- Mantenere offline le workstation (EWS) quando non necessarie

Mitigazioni

Proposte

- Firewall setup sul perimetro esposto di `VLAN 10.0.28.0/24` e `VLAN 192.168.2.0/24`
- Revisione della politica di segmentazione, come in paradigma *"zones and conduits"* di `IEC 62443`
- Correggere la violazione dell'uso di IP pubblici come privati
- Mantenere offline le workstation (EWS) quando non necessarie

Asset

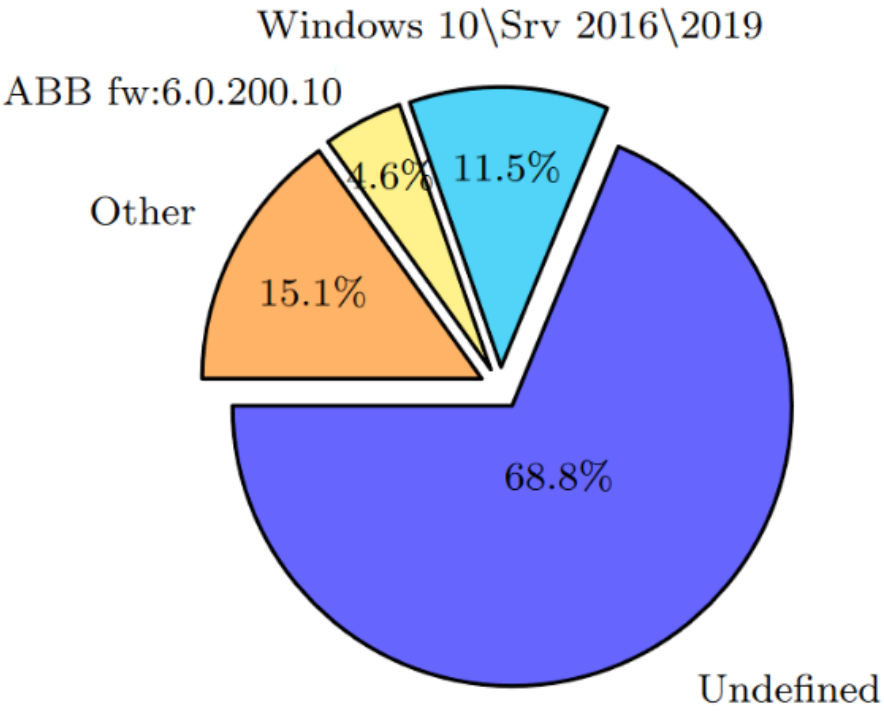


Figure: Impianto 2

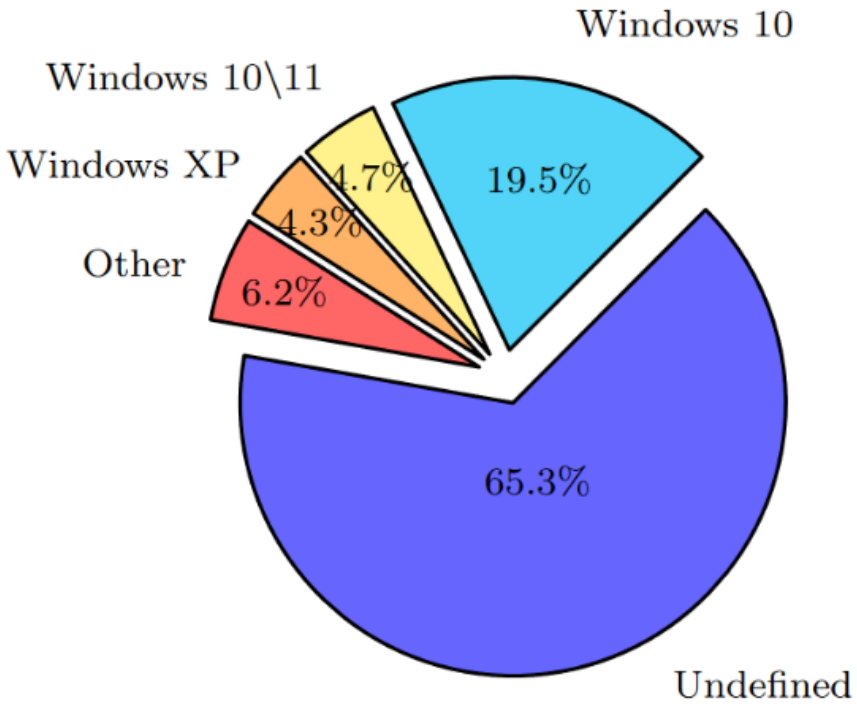


Figure: Impianto 3

Protocolli

Protocol	*Link Count*
smb	246
llmnr	116
netbios-ns	113
dce-rpc	113
dns	113
rnrp	110
igmp	91
http	86
ssdp	82
cotp	76
Not specified	315
Other	260

Figure: Impianto 2

Protocol	*Link Count*
http	120
netbios-ns	73
igmp	71
ssh	53
modbus	49
dns	45
ssdp	40
browser	33
rdp	28
llmnr	20
Not specified	74
Other	156

Figure: Impianto 3

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Mitigazioni

Proposte impianto 2

- Completare il setup per del mirroring del traffico
- Revisionare la policy di connessione delle EWS
- Implementazione di una infrastruttura centralizzata per il patching - WSUS (Windows Server Update Services)
- Disabilitare la retrocompatibilità con versioni obsolete di MS SMB
- Modificare la management policy delle allerte

Indice

Conclusioni

La situazione risulta critica. Soprattutto per il secondo e terzo impianto, rimane necessario un ampliamento del mirroring del traffico per delineare un asset inventory completo.

Lavori futuri

Considerando i protocolli e i sistemi impiegati, per il futuro si propone:

- Rafforzamento perimetrale tramite firewall (whitelist) e cambio a VPN con MFA
- Segmentazione delle reti seguendo il paradigma 'zones and conduits'
- Verifica di access control e separazione dei privilegi sul processo di monitoraggio e controllo remoto
- Mappatura del Basic Control sul processo fisico per poter offrire una metrica di criticità dell'asset

Lavori futuri

Considerando i protocolli e i sistemi impiegati, per il futuro si propone:

- Rafforzamento perimetrale tramite firewall (whitelist) e cambio a VPN con MFA
- Segmentazione delle reti seguendo il paradigma 'zones and conduits'
- Verifica di access control e separazione dei privilegi sul processo di monitoraggio e controllo remoto
- Mappatura del Basic Control sul processo fisico per poter offrire una metrica di criticità dell'asset

Lavori futuri

Considerando i protocolli e i sistemi impiegati, per il futuro si propone:

- Rafforzamento perimetrale tramite firewall (whitelist) e cambio a VPN con MFA
- Segmentazione delle reti seguendo il paradigma 'zones and conduits'
- Verifica di access control e separazione dei privilegi sul processo di monitoraggio e controllo remoto
- Mappatura del Basic Control sul processo fisico per poter offrire una metrica di criticità dell'asset

Lavori futuri

Considerando i protocolli e i sistemi impiegati, per il futuro si propone:

- Rafforzamento perimetrale tramite firewall (whitelist) e cambio a VPN con MFA
- Segmentazione delle reti seguendo il paradigma 'zones and conduits'
- Verifica di access control e separazione dei privilegi sul processo di monitoraggio e controllo remoto
- Mappatura del Basic Control sul processo fisico per poter offrire una metrica di criticità dell'asset

Lavori futuri

Considerando i protocolli e i sistemi impiegati, per il futuro si propone:

- Rafforzamento perimetrale tramite firewall (whitelist) e cambio a VPN con MFA
- Segmentazione delle reti seguendo il paradigma 'zones and conduits'
- Verifica di access control e separazione dei privilegi sul processo di monitoraggio e controllo remoto
- Mappatura del Basic Control sul processo fisico per poter offrire una metrica di criticità dell'asset

An overview of ICS vulnerabilities, threats, and security measures

Based on three real-world power plants security concerns

Silvio Ranise
Relatore

Riccardo Gennaro
Studente

UNIVERSITÀ DI TRENTO

Corso di Laurea in Informatica

Trento, 2 dicembre 2022