



SPETT. LE PAOLO RAMPINO
02 SETTEMBRE 2024

**PREVENTIVO
THETA
BY
WOLF ETHICAL
HACKERS**



WOLF ETHICAL HACKERS

PREVENTIVO INFRASTRUTTURA IT



PRIORITY -> SECURITY

ADVANCE SECURITY

LA SICUREZZA E' IL NOSTRO MESTIERE

OBIETTIVI



La scelta dei materiali e delle soluzioni tecnologiche è stata guidata dalla necessità di creare un'infrastruttura IT che sia non solo all'altezza delle attuali esigenze aziendali, ma che possa anche crescere e adattarsi a futuri sviluppi. La scalabilità è garantita dai dispositivi Cisco, che offrono funzionalità avanzate e una facile espansione della rete. La velocità è assicurata dall'uso di tecnologie di cablaggio all'avanguardia e da dispositivi di archiviazione ottimizzati. Infine, la sicurezza è al centro di questa configurazione, con firewall di nuova generazione che proteggono l'azienda da minacce esterne e interne, garantendo così la continuità operativa e la protezione dei dati.



PROPOSTA CLIENTE LEASING

1

Struttura dell'edificio è su 6 piani

2

Dispositivi totali 120 computer in leasing per 60 mesi

3

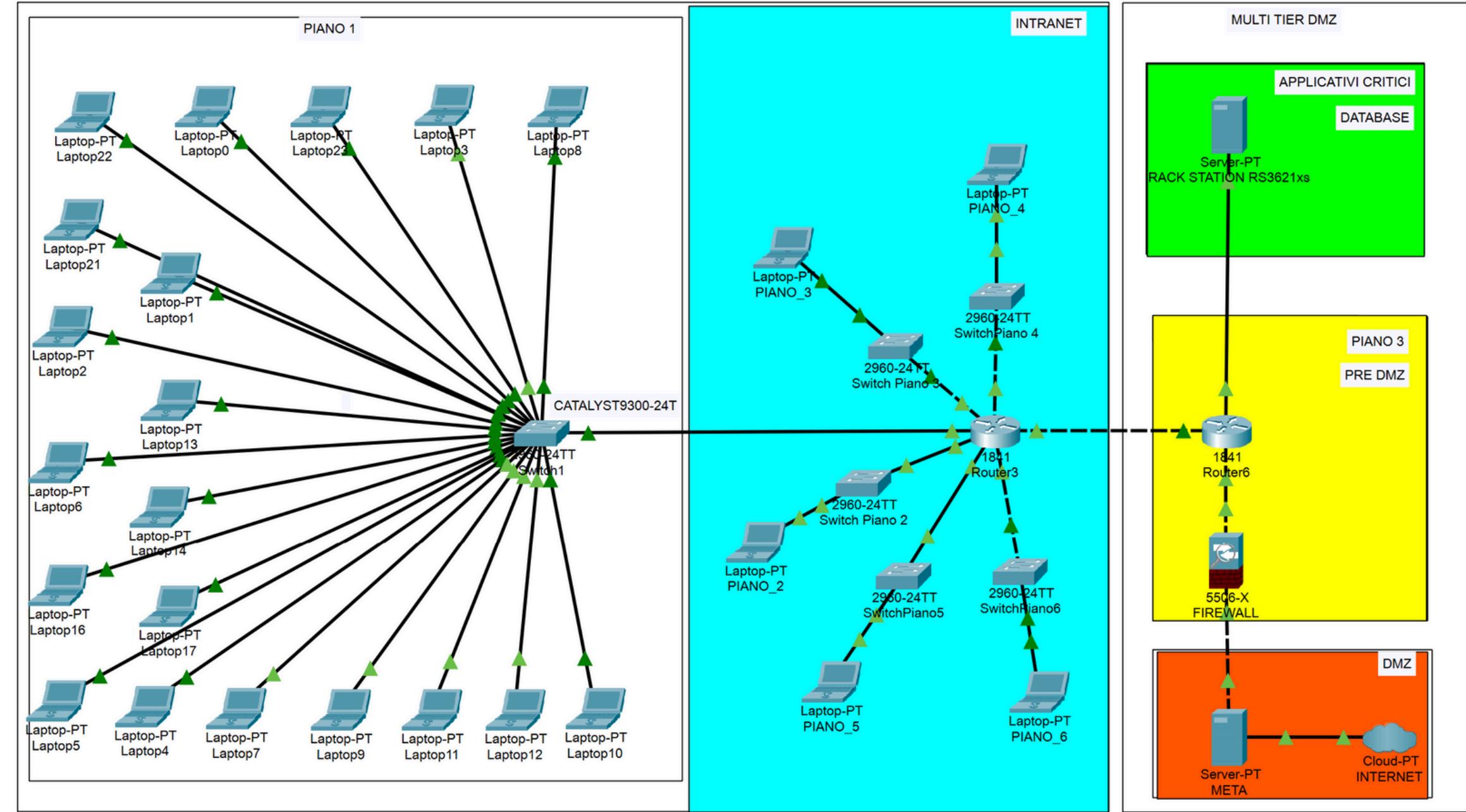
Componenti aggiuntivi:

- web server
- firewall perimetrale
- NAS
- 3 ids/ips

RETE

Analisi degli asset critici della rete proposta dal cliente.

- Frammentazione della rete, creando un Multi-Tier suddiviso in:
- Intranet (rete interna)
- Applicativi critici
- Pre-DMZ
- DMZ



Piano

- Tutti i 20 PC del piano sono collegati a uno switch.
- Lo switch indirizza il traffico verso il router centrale che è al 3 piano.

Intranet

Router/IDS

- Collegato a un altro router/IDS (CISCO ASR 1002-HX) che separa il traffico tra DMZ e Database.
- Questa separazione garantisce maggiore sicurezza, evitando l'esposizione del database al traffico esterno.

Piano 3

Sicurezza

- Tutto il sistema è protetto da un Firewall fisico/IPS.
- Router/IDS (CISCO ASR 1002-HX) che controlla il traffico interno.
- Il firewall blocca il traffico esterno verso l'Intranet.
- Agisce attivamente contro minacce e intrusioni provenienti dalla rete esterna.

Applicativi Critici

Database

- Fornisce servizi e indirizzi IP a tutti i dispositivi interni tramite il protocollo DHCP.
- Configurato per impedire l'eliminazione, il caricamento e la modifica dei dati.
- Il router/IDS notificherà all'amministratore in caso di tentativi di manomissione.



PROPOSTA 1: LEASING TERMINALI

Hardware	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop in leasing (DELL XPS – iCore 7)	120	4.245,60	509.472,00 (in 60 mesi)
Synology RackStation RS3621xs+	1	4.600	4.600
HDD Red	5	376	1.880
Cisco Firepower 2120	1	1.998	1.998
Switch Cisco Catalyst 9300-24T-E	6	1.875	11.250
Cisco ASR 1002-HX	1	29.995	29.995
Cisco 3120 NGFW	1	28.487,30	28.487,30
Totale Hardware Ivato			587.682,30



SERVIZI EXTRA 1

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Cablaggio Cat8 (per 120 computer)	1800 metri	4,50	8100,00
Connettori RJ45	240	0,50	120,00
Pannelli di Patch	6	150,00	900,00
Installazione Firewall	1	200,00	200,00
Installazione Router	1	200,00	200,00
Installazione Switch	6	150,00	900,00
Installazione IPS	3	250,00	750,00
Manodopera per Installazione PC	120 ore	50,00	6.000,00
Manodopera per Configurazione Rete	80 ore	70,00	5.600,00
Totale Manodopera e Cablaggio Ivato			22.770,00

- TOTALE HARDWARE + MANODOPERA: 610.452,30 €
- ASSISTENZA ANNUALE (10%) COSTO STIMATO: 61.045,23 €
- TOTALE OPZIONE 1 CON ASSISTENZA ANNUALE: 671.497,53 €

PROPOSTA CLIENTE ACQUISTO

1

Struttura dell'edificio è su 6 piani

2

Dispositivi totali 120 computer - Dell Latitude i7

3

Componenti aggiuntivi:

- web server
- firewall perimetrale
- NAS
- 3 ids/ips



PROPOSTA 2: ACQUISTO TERMINALI

Hardware	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop in leasing (DELL XPS – iCore 7)	120	1.100,00	132.000,00
Synology RackStation RS3621xs+	1	4.600,00	4.600,00
HDD Red	5	376,00	1.880,00
Cisco Firepower 2120	1	1.998,00	1.998,00
Switch Cisco Catalyst 9300-24T-E	6	1.875,00	11.250,00
Cisco ASR 1002-HX	1	29.995,00	29.995,00
Cisco 3120 NGFW	3	28.487,30	85.461,89
Totale Hardware			266.184,89

SERVIZI EXTRA 2

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Cablaggio Cat8 (per 120 computer)	1800 metri	4,50	8100,00
Connettori RJ45	240	0,50	120,00
Pannelli di Patch	6	150,00	900,00
Installazione Firewall	1	200,00	200,00
Installazione Router	1	200,00	200,00
Installazione Switch	6	150,00	900,00
Installazione IPS	3	250,00	750,00
Manodopera per Installazione PC	120 ore	50,00	6.000,00
Manodopera per Configurazione Rete	80 ore	70,00	5.600,00
Totale Manodopera e Cablaggio Ivato			22.770,00

- TOTALE HARDWARE + MANODOPERA: 232.980,30 €
- ASSISTENZA ANNUALE (10%) COSTO STIMATO: 23298,03 €
- TOTALE OPZIONE 1 CON ASSISTENZA ANNUALE: 256.278,33 €





PROPOSTA CLIENTE PRO ADVISOR

1

Struttura dell'edificio è su 6 piani

2

Dispositivi totali 120 computer - Dell Latitude i7

3

Componenti aggiuntivi:

- web server
- 2 firewall perimetrali
- 2 router
- NAS
- 5 ids/ips

PROPOSTA 3: PRO ADVISOR

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop (acquisto + licenze + antivirus)	120	1100	132.000,00
Synology RackStation RS3621xs+	1	4.600,00	4.600,00
HDD Red	5	376,00	1.880,00
Firepower 2120	2	1.998,00	3.996,00
Switch Cisco Catalyst 9300-24T-E	6	1.875,00	11.250,00
Cisco ASR 1002-HX (IVA inclusa)	2	29.995,00	59.990,00
Cisco 3120 NGFW	1	28.487,30	28.487,30
Totale Hardware Ivato			242.203,30



SERVIZI EXTRA 3

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Cablaggio Cat8 (per 120 computer)	1800 metri	4,50	8100,00
Connettori RJ45	240	0,50	120,00
Pannelli di Patch	6	150,00	900,00
Installazione Firewall	1	200,00	200,00
Installazione Router	1	200,00	200,00
Installazione Switch	6	150,00	900,00
Installazione IPS	3	250,00	750,00
Manodopera per Installazione PC	120 ore	50,00	6.000,00
Manodopera per Configurazione Rete	80 ore	70,00	5.600,00
Totale Manodopera e Cablaggio Ivato			22.770,00

- TOTALE HARDWARE + MANODOPERA: 264.973,30 €
- ASSISTENZA ANNUALE (10%) COSTO STIMATO: 26.497,33 €
- TOTALE OPZIONE 1 CON ASSISTENZA ANNUALE: 291.470,63 €



PROPOSTA CLIENTE WOLF ELITE

1

Struttura dell'edificio è su 6 piani

2

Dispositivi totali 120 computer - Dell Latitude i7

3

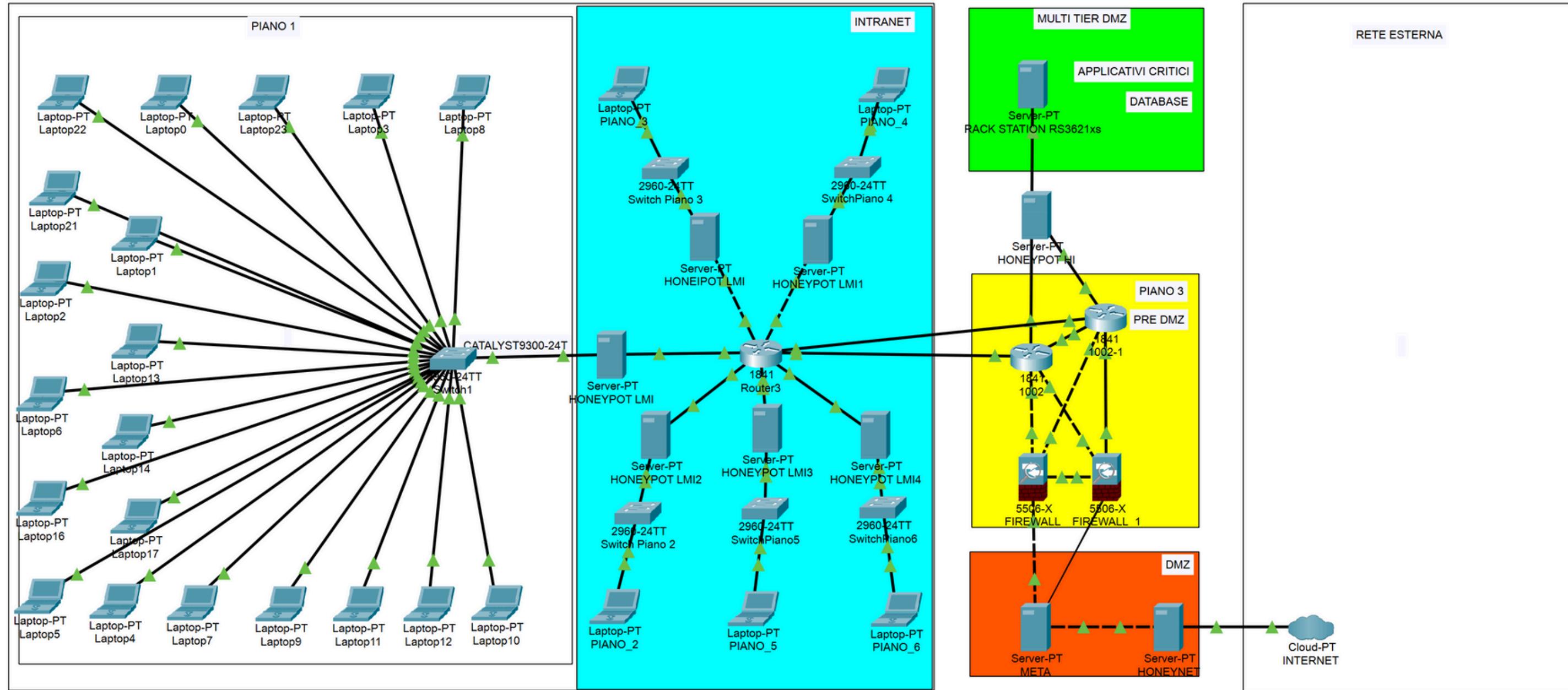
Componenti aggiuntivi:

- web server
- 2 firewall perimetrali
- 2 router
- NAS
- 5 ids/ips
- Layered Honeypots
- Honeynet

RETE

Analisi degli asset critici della rete proposta al cliente.

- Frammentazione della rete, creando un Multi-Tier suddiviso in:
- Intranet (rete interna)
- Applicativi critici
- Pre-DMZ
- DMZ
- Ridondanza Router e Firewall
- Layer Honeypots e Honeynet



Piano

- Tutti i 20 PC del piano sono collegati a uno switch.
- Lo switch indirizza il traffico verso il router centrale che è al 3 piano.

Intranet

Router/IDS

- Collegato a un altro router/IDS (CISCO ASR 1002-HX) che separa il traffico tra DMZ e Database.
- Questa separazione garantisce maggiore sicurezza, evitando l'esposizione del database al traffico esterno.

Piano 3

Sicurezza

- Tutto il sistema è protetto da un Firewall fisico/IPS.
- Router/IDS (CISCO ASR 1002-HX) che controlla il traffico interno.
- Il firewall blocca il traffico esterno verso l'Intranet.
- Agisce attivamente contro minacce e intrusioni provenienti dalla rete esterna.

Applicativi Critici

Database

- Fornisce servizi e indirizzi IP a tutti i dispositivi interni tramite il protocollo DHCP.
- Configurato per impedire l'eliminazione, il caricamento e la modifica dei dati.
- Il router/IDS notificherà all'amministratore in caso di tentativi di manomissione.



PROPOSTA WOLF ELITE: ACQUISTO TERMINALI

Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Laptop (acquisto + licenze + antivirus)	120	1100	132.000,00
Synology RackStation RS3621xs+	1	4.600,00	4.600,00
HDD Red	5	376,00	1.880,00
Firepower 2120	2	1.998,00	3.996,00
Switch Cisco Catalyst 9300-24T-E	6	1.875,00	11.250,00
Cisco ASR 1002-HX (IVA inclusa)	2	29.995,00	59.990,00
Cisco 3120 NGFW	1	28.487,30	28.487,30
Total Hardware IVA			242.203,30

SERVIZI EXTRA WOLF ELITE



Elemento	Quantità	Prezzo Unitario (€)	Totale (€)
Cablaggio Cat8 (per 120 computer)	1800 metri	4,50	8.100,00
Connettori RJ45	240	0,50	120,00
Pannelli di Patch	6	150,00	900,00
Installazione Firewall	1	200,00	200,00
Installazione Router	1	200,00	200,00
Installazione Switch	6	150,00	900,00
Installazione IPS	3	250,00	750,00
Manodopera per Installazione PC	120 ore	50,00	6.000,00
Manodopera per Configurazione Rete	80 ore	70,00	5.600,00
Honeypot a bassa interazione	6	500,00	3.000,00
Honeypot a media interazione	2	1.000,00	2.000,00
Honeypot ad alta interazione	2	2.500,00	5.000,00
Implementazione Honeynet interna	1	8.000,00	8.000,00
Totale Manodopera e Cablaggio Ivato			40.770,00



PROPOSTA WOLF ELITE LONG SUPPORT

- 1**
- 2**
- 2**

- Totale Hardware + Manodopera:

€ 264.973,30

- Assistenza Annuale inclusa

Formazione Periodica (10%):

€ 26.497,33

"Proteggiamo il tuo futuro con un servizio che non si ferma mai."

"Sicurezza garantita, con aggiornamenti costanti e formazione inclusa."

- Totale Complessivo:

€ 291.470,63

"Tutto quello di cui hai bisogno per essere al sicuro, oggi e domani."

"Investi nella tranquillità, con un sistema progettato per resistere alle minacce."

CISCO FIREPOWER 2120

Descrizione Generale

- Firewall di nuova generazione progettato per offrire protezione avanzata contro minacce e intrusi.
- Soluzione integrata di sicurezza che combina:
- Prevenzione delle Intrusioni (IPS)
- Protezione avanzata contro malware
- Filtraggio dei contenuti

Layer di Riferimento OSI

- Layer 2 (Data Link):
- Supporta bridging e switch per il monitoraggio del traffico sulla rete.
- Layer 3 (Network):
- Include routing, filtraggio IP, NAT e segmentazione della rete.
- Layer 4 (Transport):
- Filtra il traffico basato su protocolli come TCP e UDP.
- Layer 7 (Application):
- Ispezione e controllo del traffico applicativo (HTTP, HTTPS, ecc.).

Funzionalità Principali

- Prevenzione delle Intrusioni (IPS):
 - Blocca minacce note e sconosciute in tempo reale.
- Advanced Malware Protection (AMP):
 - Protezione contro malware avanzato con funzionalità di sandboxing.
- URL Filtering:
 - Controllo dell'accesso ai siti web basato su categorie predefinite.
- VPN (Virtual Private Network):
 - Supporta connessioni VPN sicure per accesso remoto.

Scalabilità e Prestazioni

- Progettato per piccole e medie imprese, scalabile con l'aumento delle esigenze di sicurezza.
- Prestazioni firewall fino a 3 Gbps, supporta migliaia di connessioni simultanee.

CISCO ASR 1002-HX ROUTER

Descrizione Generale

- Il Cisco ASR 1002-HX è un router di fascia alta progettato per gestire grandi volumi di traffico dati e garantire alta disponibilità. È ideale per reti aziendali che richiedono prestazioni elevate e funzionalità avanzate di routing.

Layer di Riferimento OSI

- Layer 2 (Data Link):
 - Supporta tecnologie WAN come Ethernet, MPLS, e Frame Relay.
- Layer 3 (Network):
 - Implementa protocolli di routing dinamico come OSPF, BGP, e EIGRP per la gestione avanzata del traffico IP.
- Layer 4 (Transport):
 - Gestisce il traffico TCP/UDP con funzionalità avanzate di QoS (Quality of Service) e load balancing.
- Layer 7 (Application):
 - Supporta servizi di rete avanzati, come deep packet inspection (DPI) e servizi applicativi integrati.

Funzionalità Principali

- Routing Dinamico:
- Supporta protocolli di routing avanzati per gestire il traffico in modo efficiente.
- QoS (Quality of Service):
 - Permette di prioritizzare il traffico di rete critico per applicazioni specifiche, garantendo prestazioni ottimali.
- VPN:
 - Supporta VPN su larga scala con capacità di cifratura hardware.
- High Availability:
 - Include funzionalità di ridondanza e failover per garantire alta disponibilità.

Scalabilità e Prestazioni

- Supporta fino a 200 Gbps di throughput aggregato.
- Capacità di gestire milioni di pacchetti al secondo, ideale per ambienti ad alta intensità di dati.

SWITCH CISCO CATALYST 9300-24T-E

Descrizione Generale

- Il Cisco Catalyst 9300-24T-E è uno switch di rete di fascia enterprise, ottimizzato per la gestione di reti ad alte prestazioni. È particolarmente adatto per ambienti che richiedono alta densità di porte e funzionalità avanzate di switching.

Layer di Riferimento OSI

- Layer 2 (Data Link): Fornisce switching Layer 2 con supporto per VLAN, spanning tree, e aggregazione di link.
- Layer 3 (Network): Include funzionalità di routing inter-VLAN, routing statico e dinamico.
- Layer 4 (Transport): Supporta QoS e ACL (Access Control Lists) per il controllo avanzato del traffico.

Funzionalità Principali

- Stacking: Supporta l'empilamento fisico fino a 8 switch, permettendo la gestione centralizzata e l'espansione della rete.
- Supporto per SD-Access: Integrato con Cisco DNA, consente la gestione automatizzata della rete e la segmentazione basata su policy.
- Security Features: Include Cisco TrustSec per la segmentazione della rete e la protezione delle risorse aziendali.
- Power over Ethernet (PoE): Alimenta dispositivi come telefoni IP e access point wireless direttamente tramite le porte Ethernet.

Scalabilità e Prestazioni

- Progettato per supportare fino a 24 porte 10 Gbps, con capacità di aggregazione fino a 480 Gbps.
- Supporta applicazioni ad alta densità di banda, ideale per ambienti aziendali complessi.

HONEYPOTS

1. Honeypot a bassa e media interazione:

- Posizione: Distribuiti sui vari piani, in prossimità dei 6 switch Cisco Catalyst 9300-24T-E, vicino ai computer e in punti strategici della rete.
- Obiettivo: Rilevare attacchi comuni e automatizzati, come tentativi di accesso non autorizzato agli switch o attacchi alle interfacce di rete esposte.

2. Honeypot ad alta interazione:

- Posizione: Prossimo al router Cisco ASR 1002-HX e al NAS Synology RS3621xs+. Questi honeypot saranno più realistici e saranno posizionati per attirare attacchi sofisticati diretti a infrastrutture critiche come il vostro NAS o router aziendale.
- Obiettivo: Monitorare tentativi di compromissione più avanzati e tecniche di persistenza da parte di attaccanti più qualificati.

HONEYNET

3. Honeynet interna:

- Posizione: Simulerà un'intera rete interna, comprensiva di servizi vulnerabili come il server aziendale con DVWA e Metasploit, creando un ambiente che attira attacchi complessi e avanzati.
- Obiettivo: Raccogliere dati su tecniche di movimento laterale e tentativi di sfruttamento all'interno della rete, simulando una compromissione completa dell'infrastruttura.

4. Monitoraggio centralizzato e gestione dei log:

- Un sistema centralizzato raccoglierà i log di tutte le interazioni sugli honeypot e sulla honeynet. Potrà essere integrato con strumenti come Elastic Stack o Splunk, permettendo una gestione efficiente e in tempo reale dei dati generati.

SYNOLOGY RACKSTATION RS3621XS CON HDD WD RED PRO 10 TB

Synology RackStation RS3621xs+

- Il Synology RackStation RS3621xs+ è una soluzione NAS (Network Attached Storage) di fascia alta, progettata per fornire una gestione centralizzata dei dati. Offre prestazioni elevate con una capacità di espansione flessibile, ideale per aziende che necessitano di un'archiviazione sicura e scalabile. Supporta fino a 12 drive, con un'architettura potente per gestire carichi di lavoro intensivi.

Western Digital Red Pro 10 TB

- Il WD Red Pro 10 TB è un hard disk ottimizzato per l'uso in ambienti NAS, progettato per garantire affidabilità e prestazioni elevate. Ideale per carichi di lavoro intensivi, offre una capacità di archiviazione significativa con una velocità di trasferimento dati ottimizzata per le configurazioni multi-drive. Perfetto per le aziende che necessitano di una soluzione di archiviazione robusta e duratura.

CISCO 3120 NGFW (NEXT GENERATION FIREWALL)

Cisco 3120 NGFW (Next Generation Firewall)

- Il Cisco 3120 NGFW è stato selezionato per rafforzare ulteriormente la sicurezza della rete aziendale. Con la sua capacità di ispezione approfondita dei pacchetti (DPI), protezione contro le intrusioni e monitoraggio continuo delle minacce, questo firewall offre una protezione multilivello che è fondamentale per un'azienda che si affida a operazioni sicure e ininterrotte. La sua scalabilità e capacità di gestione del traffico ad alte prestazioni lo rendono ideale per un ambiente in cui la sicurezza non può essere compromessa.



ANALISI FORENSE

1

Scansione porte su META

2

Scansione verbi HTTP

3

File Zip Steganografia

SCANSIONE PORTE

PORTE COMUNEMENTE UTILIZZATE E POTENZIALI RISCHI

Porta 21: FTP (File Transfer Protocol) – non sicura, usa SFTP sulla porta 22 se possibile.
Porta 22: SSH (Secure Shell) – sicura, ma deve essere monitorata per evitare accessi non autorizzati.
Porta 23: Telnet – altamente insicura, da evitare o sostituire con SSH.
Porta 25: SMTP (Simple Mail Transfer Protocol) – usata per l'invio di email, può essere sfruttata per spam.
Porta 53: DNS (Domain Name System) – essenziale, ma può essere target di attacchi DDoS o avvelenamento DNS.
Porta 80: HTTP (HyperText Transfer Protocol) – traffico web non criptato, meglio utilizzare HTTPS sulla porta 443.
Porta 111: RPC (Remote Procedure Call) – vulnerabile a exploit remoti.
Porta 135: Microsoft RPC – legata a vulnerabilità di Windows come attacchi DCOM.
Porta 137-139: NetBIOS – associata a condivisione file su reti Windows, vulnerabile a exploit.
Porta 443: HTTPS (HyperText Transfer Protocol Secure) – porta per traffico web criptato, da lasciare aperta solo con certificati validi.
Porta 445: SMB (Server Message Block) – bersaglio di malware come WannaCry.
Porta 3389: RDP (Remote Desktop Protocol) – vulnerabile a brute force e exploit se non ben protetta

ALTRÉ PORTE COMUNI A CUI PRESTARE ATTENZIONE

Porta 5900: VNC (Virtual Network Computing) – utilizzata per accessi remoti, da proteggere adeguatamente.
Porta 3306: MySQL – database, da proteggere con firewall e accessi limitati.
Porta 5432: PostgreSQL – simile a MySQL, va ben protetta.

PORTE SPECIFICHE

Porta 23 (Telnet): Insicura e da evitare a favore di SSH.
Porta 512-514: Rlogin/Rsh – protocolli vecchi e insicuri, da evitare.
Porta 6667: IRC (Internet Relay Chat) – può essere usata per canali di comando e controllo dei bot.
Porta 8080, 8180: HTTP alternativo o applicazioni di sviluppo.

SCANSIONE HTTP

PROBLEMATICHE CON PUT E DELETE

- PUT (200): Questo può essere un segnale di allarme. Il metodo PUT è spesso utilizzato per aggiornare risorse sul server. Se è abilitato senza limitazioni adeguate, un utente malintenzionato potrebbe potenzialmente modificare dati sensibili o caricare file dannosi.
- DELETE (200): Anche questo è preoccupante. Il metodo DELETE dovrebbe essere molto ben controllato. Se un attaccante riesce a inviare richieste DELETE senza restrizioni, potrebbe potenzialmente eliminare dati importanti.

RISCHI

- phpMyAdmin esposto: Se phpMyAdmin è accessibile pubblicamente con questi verbi HTTP abilitati, è necessario assicurarsi che l'accesso sia adeguatamente protetto con autenticazione e restrizioni IP.
- Test PUT e DELETE: Questi metodi dovrebbero essere bloccati se non strettamente necessari, soprattutto su endpoint critici.

AZIONI CONSIGLIATE

- Assicurarsi che l'accesso a phpMyAdmin sia protetto da autenticazione e che sia visibile solo a chi ne ha bisogno (ad esempio, limitando l'accesso tramite firewall o VPN).
- Disabilita i metodi PUT e DELETE a meno che non siano necessari e configura le opportune regole di autenticazione e autorizzazione per l'uso di questi metodi.
- Verifica la corretta validazione e filtraggio delle richieste POST, PUT e DELETE per prevenire attacchi come SQL injection, file upload malevolo o cancellazione non autorizzata di dati.

SCANSIONE FILE ZIP

PROBLEMATICA CON FILE THETA

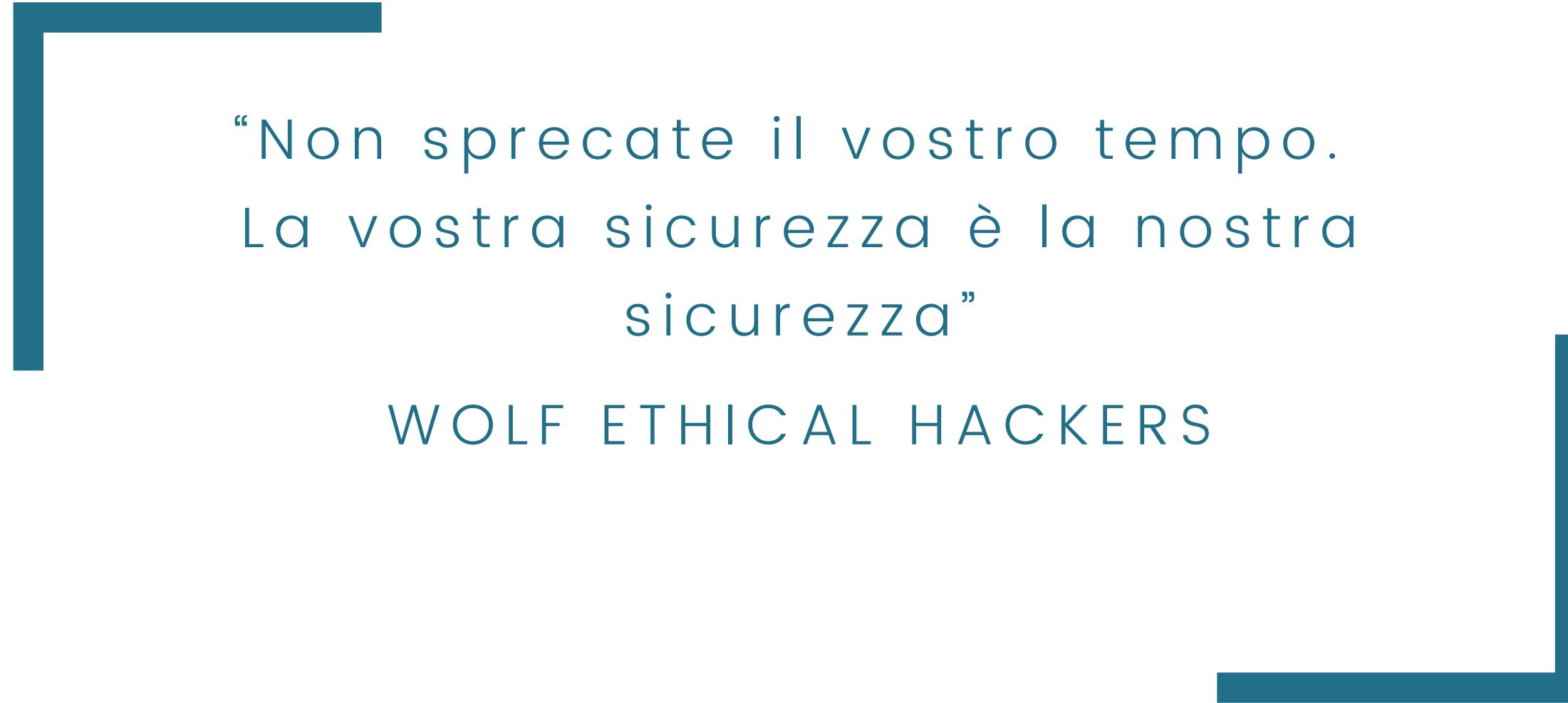
L'amministratore delegato ci ha consegnato un file zip chiamato 'THETA'. A una prima verifica, tutto sembrava normale.

Tuttavia, il team di Wolf Ethical Hackers ha notato qualcosa di strano nelle dimensioni dei file jpg all'interno.

Utilizzando il tool Steghide, hanno scoperto che questi file erano cifrati con l'uso di linguaggi esoterici, come Brainfuck e Cow language.

Inoltre, i file decodificati in base64 rivelavano un altro file che conteneva un messaggio criptato.

All'interno del file 'text.txt' si leggeva: 'Abbiamo svuotato i conti, grazie azienda Theta!'.



“Non sprecate il vostro tempo.
La vostra sicurezza è la nostra
sicurezza”

WOLF ETHICAL HACKERS



WOLF ETHICAL HACKERS S.R.L



- ANDREA BRANDI



- ANGELO LOMBARDI



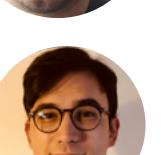
- FRANCESCO LETO



- MATTIA DELEU



- MICHELE GUIDO



- NICOLO' BIASIO



- SUSHANTO ROMA

CONTATTI

“Realizziamo insieme
la tua sicurezza”





GRAZIE

WOLF ETHICAL HACKERS