Security First

Vogliamo tenere i criminali a chilometri dalla vostra rete!

INFONET
NETWORKING & COMMUNICATION

8000 dipendenti pubblici a carta e penna

Gli hacker bloccano Atlanta!

LA STAMPA

Un attacco hacker ha bloccato la città di Atlanta

Per cinque giorni, un ransomware ha colpito i computer di 8mila dipendenti pubblici

Durato cinque giorni e terminato giovedì 29 marzo, L'attacco ha colpito i sistemi informatici della corte di giustizia, dell'amministrazione comunale e dei centri per l'impiego. 8mila dipendenti pubblici **non hanno potuto accendere i computer e per lavorare hanno dovuto utilizzare carta e penna**.

INFONET
NETWORKING & COMMUNICATION

Rubate 380.000 carte di credito

Multa da 204 Milioni a British Airways per non essersi protetta!

British Airways vittima del primo grande data breach nell'era del GDPR

di **Paolo Anastasio** | 10 Settembre 2018, ore 11:10

INFONET
NETWORKING & COMMUNICATION

Immagina se…

Può succedere a tutti, grandi e piccoli!

Si spegnessero tutti i semafori di una città

Si bloccassero tutti gli ascensori di un palazzo

Venissero rubati i dati del nostro commercialista o medico

INFONET
NETWORKING & COMMUNICATION

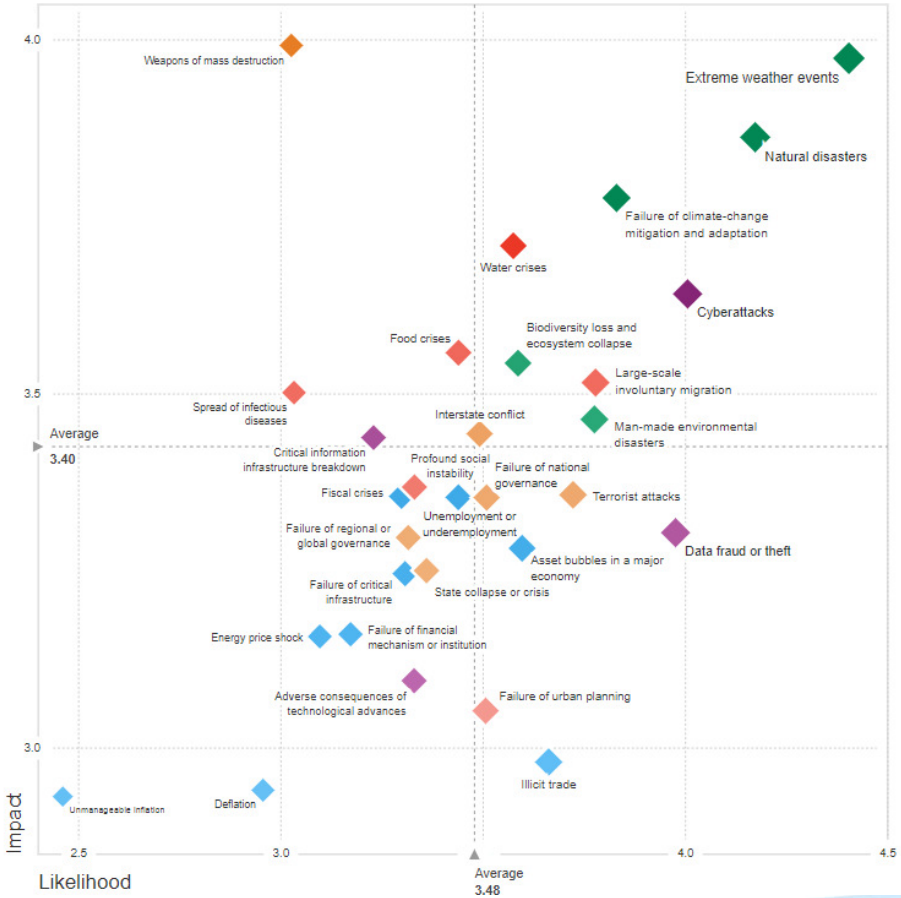
The Global Risks Report 2018

Cyber Crime? Peggio del terrorismo!

WORLD ECONOMIC FORUM

The Global Risks Landscape 2018

What is the impact and likelihood of global risks?



Top 10 risks in terms of
Likelihood

1. Extreme weather events
2. Natural disasters
3. Cyberattacks
4. Data fraud or theft
5. Failure of climate-change mitigation and adaptation
6. Large-scale involuntary migration
7. Man-made environmental disasters
8. Terrorist attacks
9. Illicit trade
10. Asset bubbles in a major economy

Top 10 risks in terms of
Impact

1. Weapons of mass destruction
2. Extreme weather events
3. Natural disasters
4. Failure of climate-change mitigation and adaptation
5. Water crises
6. Cyberattacks
7. Food crises
8. Biodiversity loss and ecosystem collapse
9. Large-scale involuntary migration
10. Spread of infectious diseases

INFONET
NETWORKING & COMMUNICATION

The Global Risks Report 2018

WORLD ECONOMIC FORUM

Un trend esplosivo!

Top 5 Global Risk in Terms of Likelihood

2016	2017	2018
Large-scale involuntary migration	Extreme weather events	Extreme weather events
Extreme weather events	Large-scale involuntary migration	Natural disasters
Failure of climate-change mitigation and adaptation	Major natural disasters	Cyberattacks
Interstate conflict with regional consequences	Large-scale terrorist attacks	Data fraud or theft
Major natural catastrophes	Massive incident of data fraud/theft	Failure of climate-change mitigation and adaptation

INFONET
NETWORKING & COMMUNICATION

Gli esperti riconoscono il problema

Ci ostiniamo a non vederlo!

I 10 macrotrends 2019

1. **Equilibri geopolitici globali.** Verso maggiori incertezze e instabilità nel quadro globale. Si accentuano i rischi geopolitici sia regionali (Medio Oriente, Siria, Iran) che globali (Usa, Cina, tensioni nella UE). Aumenta il contrasto ai grandi flussi migratori. Crescita diffusa del nazionalismo e del populismo, con affermazione dei relativi movimenti in diversi Paesi e gravi rischi di arretramento dei regimi democratici.
2. **Scenario economico mondiale.** Ulteriore allentamento degli accordi internazionali e dell'integrazione. Forte intensificazione del protezionismo e della regionalizzazione; più intensi conflitti commerciali. Pesanti rischi di una nuova crisi finanziaria.
3. **Politiche economiche.** Fine della fase di espansione monetaria e graduale irrigidimento delle politiche monetarie in tutti i Paesi. Ingessamento delle politiche fiscali, condizionate dall'alto livello dei debiti pubblici. Cresce la richiesta di contrasto alle nuove diseguaglianze.
4. **Impatto della tecnologia.** Sviluppo esponenziale delle tecnologie digitali e crescente applicazione degli strumenti e dei dispositivi connessi e intelligenti. Crescente ibridazione tra informatica e biologia. Cross-fertilizzazione inter-settoriale.
5. **Automazione.** Machine learning, robot intelligenti, intelligenza artificiale e singolarità tecnologica. I problemi etici del rapporto uomo-macchina.
6. **Cyber-sicurezza.** Aggravamento dei temi legati a sicurezza e privacy e al cyber-crime. Intensificazione delle azioni di prevenzione e contrasto con investimenti crescenti. Sale il rischio del cyber-warfare.
7. **Imprese e rivoluzione digitale.** Innovazione nei modelli di business abilitati dal digitale. Crescente adozione dei modelli *platform based*. Nuove forme di concorrenza. Effetti di *disruption* ed effetti-rete.
8. **Tecnologia, occupazione, lavoro e competenze.** Impatto di robotica e intelligenza artificiale sul lavoro. Effetti di ricomposizione nei mercati del lavoro. Potenziale incerto di disoccupazione tecnologica. Permane il mismatch delle competenze. Più forti esigenze di formazione alle new skills. Nuove modalità di apprendimento e *continuous learning*.
9. **Demografia e ambiente.** Si accentuano gli effetti sociali e finanziari dell'allungamento della vita media. Prosegue l'espansione demografica su scala mondiale accoppiata a trend di invecchiamento. Forti fenomeni di urbanizzazione e incremento delle mega-città. Nuove forme di mobilità e di condivisione.
10. **Climate Change.** Si accentuano gli effetti di *disruption* generati dal cambiamento climatico, dal riscaldamento globale e da fenomeni naturali estremi. Crescente impatto sull'economia e sulla gestione delle organizzazioni. Maggiori investimenti in decarbonizzazione, elettrificazione, energie rinnovabili, miglior uso delle risorse.

8 | SUPPLEMENTO A HARVARD BUSINESS REVIEW - NOVEMBRE 2018

INFONET
NETWORKING & COMMUNICATION

Anche l’Europa è in allerta

L’ex presidente Junker già nel 2017

La cybersecurity è la seconda emergenza in Europa, dopo il cambiamento climatico e prima dell’immigrazione. Lo ha detto il presidente della Commissione Europea Jean-Claude Junker nel discorso sullo stato dell’Unione del 13 settembre 2017.

INFONET
NETWORKING & COMMUNICATION

Pensi che non ti riguardi?

I Trend in Italia, occhio alle PMI!

% Imprese italiane che hanno subito almeno un attacco informatico nell'ultimo anno

Area geografica	
Nord Ovest	44.2
Nord Est	47,3
Centro	52,3
Sud e Isole	35,9
Numero di addetti	
20 – 49	42,7
50 – 199	48,4
200 – 499	56,0
500 e oltre	62,8

Libro Bianco della Cyber Security - Il Futuro della Cyber Security in Italia

INFONET
NETWORKING & COMMUNICATION

Attacchi DDoS

Un aumento incredibile!

CYBERSECURITY360 | Cybersecurity Nazionale | Malware e at

LA MINACCIA

Aumentano gli attacchi DDoS: + 84% nel primo trimestre 2019

DDoS Attack Size and Traffic Increasing

Peak attack size increased **174% Y/Y.***

DDoS attacks can represent up to **25%** of a country's total Internet traffic while they are occurring.

Average DDoS attack size between 1-2 Gbps increased **37% Y/Y** which is faster than Internet traffic at **33% Y/Y**.

* 1H2017-1H2018

Source: Arbor Networks, Cisco VNI Global IP Traffic Forecast, 2017-2022

INFONET
NETWORKING & COMMUNICATION

Criminali a noleggio

Il Cyber Crime paga ed è poco rischioso!

SaaS, IaaS, DBaaS…

CaaS: Crime as a Service!

RANSOMWARE-IN-A-KIT

- Gratuito
- 30% commissioni ai produttori

DDoS ON DEMAND

- Economico
- Noleggio reti compromesse
- Traffico direzionabile su target

INFONET
NETWORKING & COMMUNICATION

Investimenti in Italia

Ci ostiniamo a non curare una malattia degenerativa!

10

MILIARDI DI €

i costi in Italia nel 2017 generati dal Cybercrime [1]

1

MILIARDO DI €

gli investimenti in Italia nel 2017 in sicurezza informatica (un decimo dei costi causati dal Cybercrime!) [1]

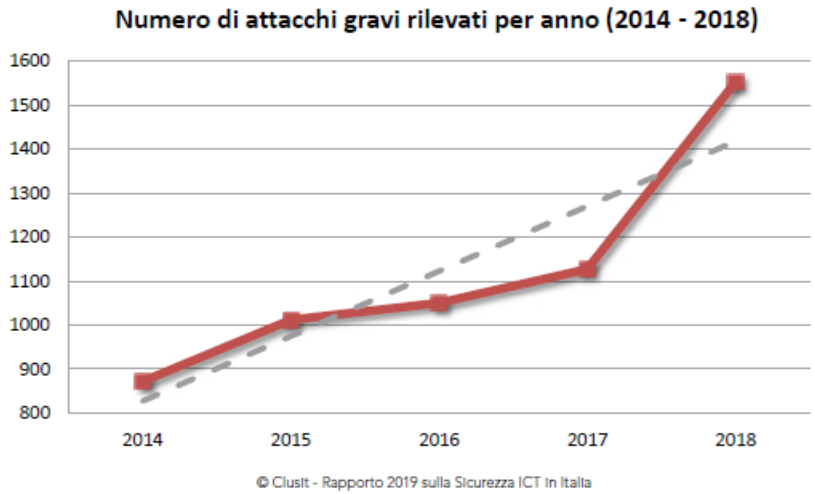
I danni sono 10 volte gli investimenti nella protezione!

(1) corrierecomunicazioni.

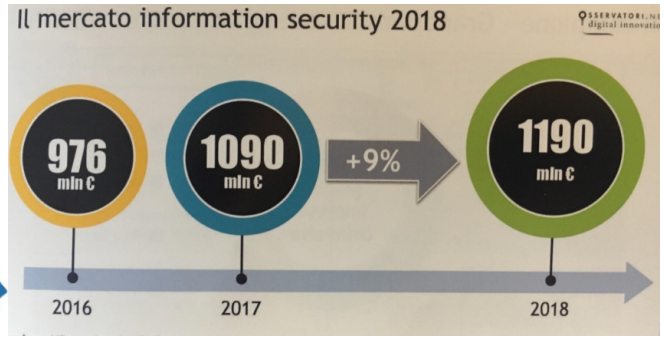
INFONET
NETWORKING & COMMUNICATION

Gli attacchi aumentano

Gli investimenti no!



Attacchi +37%
2017 su 2018



Investimenti +9%
2017 su 2018

Report Osservatorio Information Security & Privaci del Politecnico di Milano

INFONET
NETWORKING & COMMUNICATION

Utenti inconsapevoli

Informare è il primo passo!

Da una ricerca effettuata dall'Osservatorio Information Security & Privacy del Politecnico di Milano:

il **52%** delle PMI italiane sono «inconsapevoli» circa i rischi

Report Osservatorio Information Security & Privacy del Politecnico di Milano

INFONET
NETWORKING & COMMUNICATION

INFONET si è già mossa!!!!

Security First!

E NOI?

Security By Design!

Fornire connettività
già sicure

INFONET
NETWORKING & COMMUNICATION

Traffico Internet anomalo

Test tecnici dimostrano…

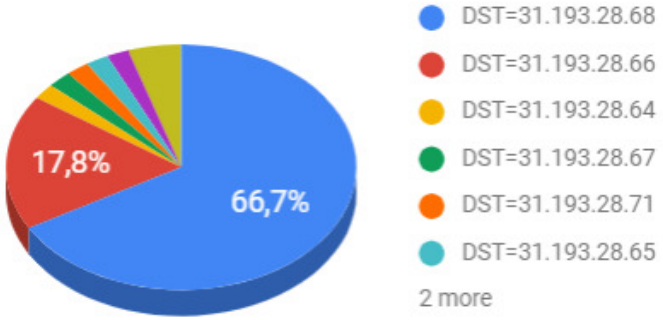
134799	ANTI_SYN_FLOOD:	SRC=185.254.122.11	DST=31.193.28.71	PROTO=TCP	SPT=47672	DPT=580
134800	PORT_SCAN:	SRC=185.254.122.11	DST=31.193.28.71	PROTO=TCP	SPT=47672	DPT=580
134801	RESERVED_CLASS:	SRC=14.225.3.37	DST=31.193.28.69	PROTO=TCP	SPT=1799	DPT=23
134802	ANTI_SYN_FLOOD:	SRC=185.251.39.73	DST=31.193.28.67	PROTO=TCP	SPT=44136	DPT=651
134803	PORT_SCAN:	SRC=185.251.39.73	DST=31.193.28.67	PROTO=TCP	SPT=44136	DPT=651
134804	ANTI_SYN_FLOOD:	SRC=185.251.39.73	DST=31.193.28.67	PROTO=TCP	SPT=44136	DPT=707
134805	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134806	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134807	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134808	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134809	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134810	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134811	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134812	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134813	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134814	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134815	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134816	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134817	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134818	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134819	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134820	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134821	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134822	ANTI_SYN_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134823	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134824	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134825	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134826	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134827	ANTI_SYN_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134828	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134829	ANTI_SYN_FLOOD:	SRC=185.254.122.116	DST=31.193.28.68	PROTO=TCP	SPT=47930	DPT=9772
134830	PORT_SCAN:	SRC=185.254.122.116	DST=31.193.28.68	PROTO=TCP	SPT=47930	DPT=9772
134831	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134832	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134833	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134834	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25
134835	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134836	ANTI_SPAM_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134837	ANTI_SYN_FLOOD:	SRC=103.231.139.146	DST=31.193.28.68	PROTO=TCP	SPT=62344	DPT=25
134838	ANTI_SPAM_FLOOD:	SRC=103.231.139.184	DST=31.193.28.68	PROTO=TCP	SPT=32640	DPT=25

log giornalieri del traffico Internet anomalo di un singolo collegamento FTTc

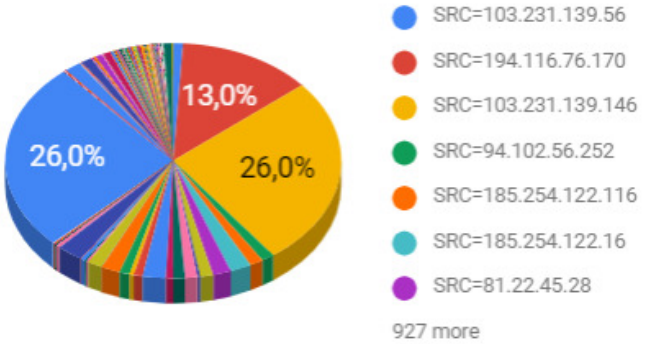
INFONET
NETWORKING & COMMUNICATION

Traffico Internet anomalo

Destination IP address



Source IP address



Filtered service

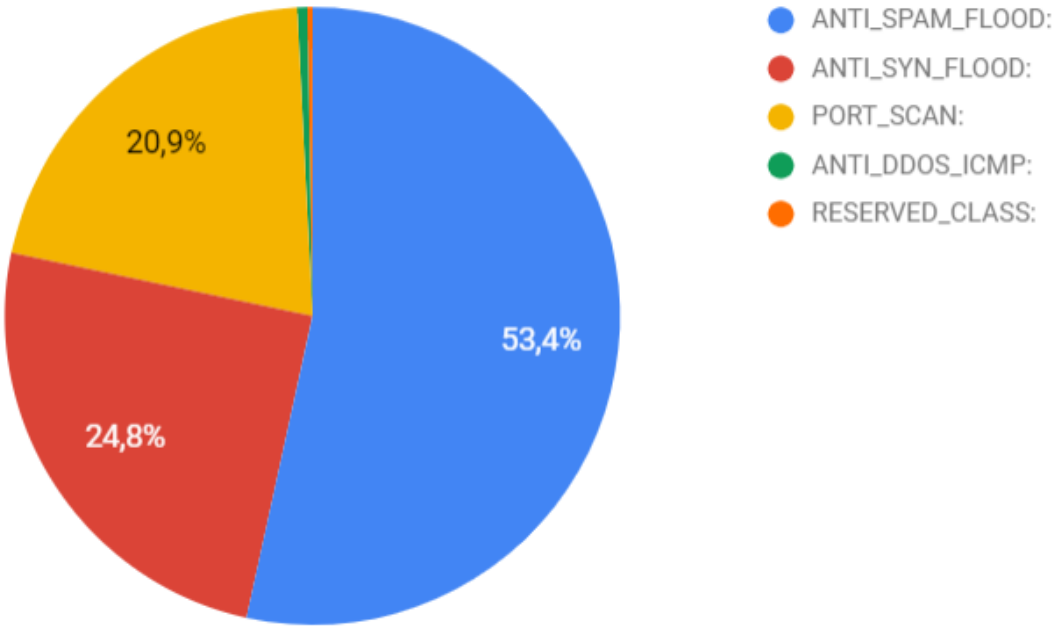


Grafico giornaliero del traffico Internet anomalo di un singolo collegamento FTTc

Security First

- Funzionalità di base
- In Cloud: a monte della sede Utente
- Rileva comportamenti anomali sulla linea
- Esclude il traffico anomalo

INFONET
NETWORKING & COMMUNICATION

Security First

Una protezione a monte

- Molte minacce sono difficili da gestire una volta arrivate alla rete dell'utente (Es. DDoS)
- Una linea, pulita da traffico malevolo, è più performante.

INFONET
NETWORKING & COMMUNICATION

Security First

Come funziona

- Attivabile e disattivabile in tempo reale da Area Riservata
- Due apparati in HA filtrano il traffico
- Se gli apparati vengono meno la connessione non ne risente, il traffico torna a essere non filtrato fino al ripristino.
- Ogni tipologia di protezione è attivabile singolarmente.
- Possiamo attivare i filtri su singoli IP o su gruppo di IP
- Sistema di White List e Black List per gestire i falsi positivi

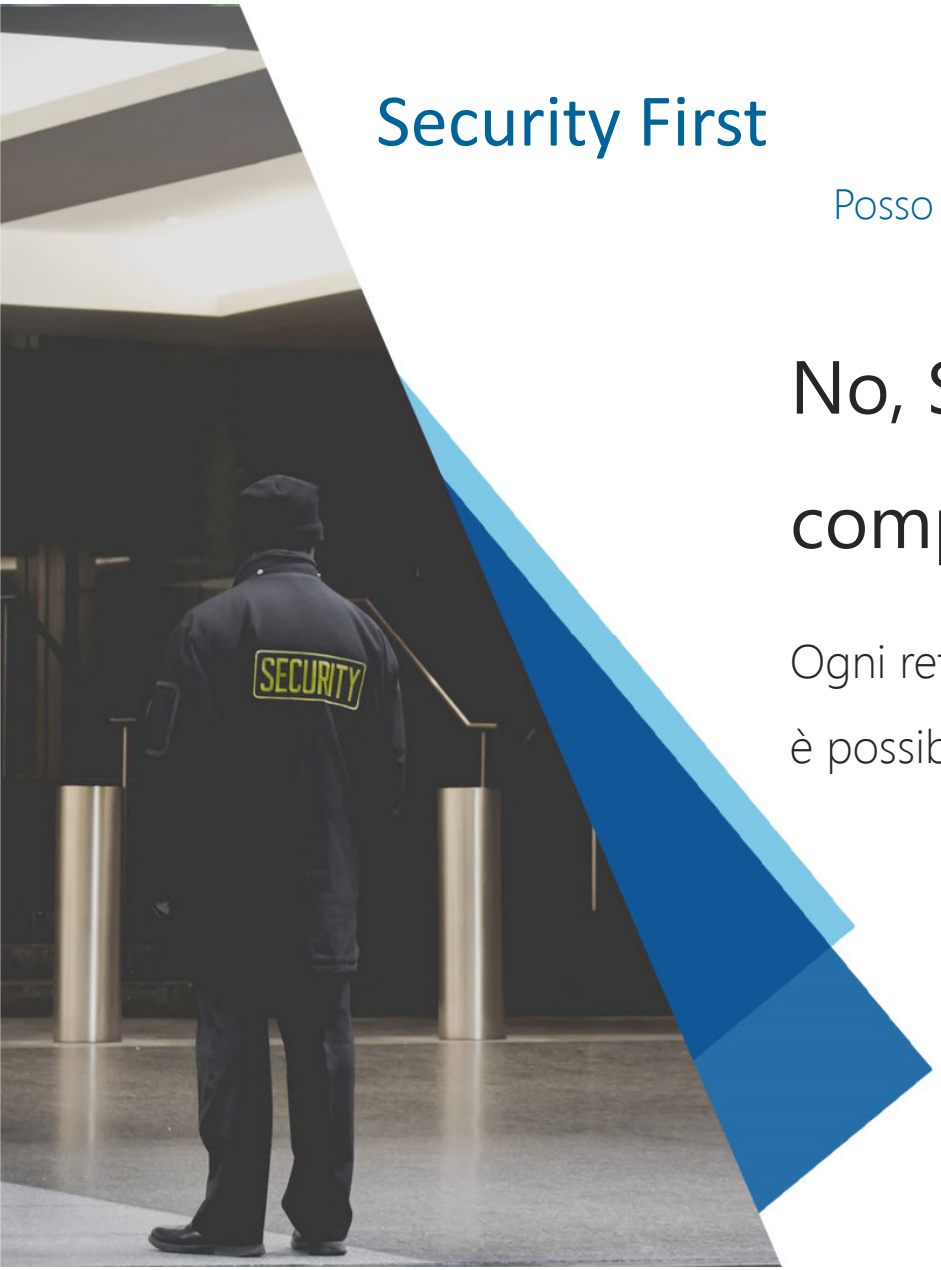
INFONET
NETWORKING & COMMUNICATION

Security First

Quali attacchi previene?

- Port-Scan
- DDoS
- Black List di IP pubblici segnalati come dannosi e continuamente aggiornati.
- Anti-flood di e-mail spamming
- Altri filtri sono in continua progettazione…

INFONET
NETWORKING & COMMUNICATION



Security First

Posso buttare il Firewall?

No, Security First e il Firewall sono complementari

Ogni rete è diversa e ogni rete ha delle esigenze specifiche che non è possibile standardizzare.

INFONET
NETWORKING & COMMUNICATION

Security First

GDPR Compliant.

- Ha superato il vaglio dell'ufficio legale
- In corso la valutazione d'impatto
- Protegge i dati da minacce esterne

Accountability

- *Dover Agire*
- *Rendere conto dell'azione fatta*

INFONET
NETWORKING & COMMUNICATION

Security First

Prospettive di sviluppo.

In progettazione un **servizio avanzato**

Per arrivare a...

- Istanze personalizzabili per Cliente
- Assessment
- Penetration Test
- Polizze Cyber Risk

INFONET
NETWORKING & COMMUNICATION

Aggiungere valore per il nostri clienti

Farlo con la Cyber Security

La scelta di proporre valore con la Cyber Security non è casuale

E' dimostrazione di interesse e responsabilità verso i nostri Clienti

INFONET
NETWORKING & COMMUNICATION

INFONET

NETWORKING & COMMUNICATION