Il ruolo del Risk Manager alla luce del COViD-19

La Security Awareness: come integrare i Cyber Risk nel programma di Risk Management

Ing. Emanuele Greco

Luglio 2020

«Fase 3» dell'emergenza coronavirus

Ripresa delle attività industriali

crisi globale nuove priorità

Luglio 2020

«Fase 3» dell'emergenza coronavirus

Ripresa delle attività industriali

crisi globale nuove priorità

Abbassamento della guardia nei confronti delle minacce informatiche

Gli hacker approfittano proprio di questo particolare momento di per diffondere le loro campagne malevole.
Nell'ultimo periodo **si riscontra un aumento degli attacchi ransomware**.


TANTO A
ME NON
CAPITA

TANTO A ME NON CAPITA

26 GIUGNO
FURTO DI INFORMAZIONI TIM

Dipendenti Tim vendevano a call center i dati dei clienti, perquisizioni e arresti

(ansa)

L'operazione Data Room della polizia postale con il coordinamento della Procura di Roma. Venti i provvedimenti cautelari. Tredici i call center individuati. Un nuovo filone di indagini ha scoperto lo stesso sistema nel settore dell'energia. L'azienda: "Ci costituiremo parte civile"

Il complesso "sistema" vedeva da un lato una serie di tecnici infedeli in grado di procacciare i dati, dall'altro una vera e propria rete commerciale che ruotava attorno alla figura di un imprenditore campano, acquirente della "merce" ed a sua volta in grado di estrarre "in proprio", anche con l'utilizzo di software di automazione, grosse quantità di informazioni, in virtù di credenziali illecitamente carpite a dipendenti ignari.
La "merce" veniva poi piazzata sul mercato dei call center, e si trattava di informazioni particolarmente appetibili per le società di vendita di contratti da remoto, che cercano per l'appunto di intercettare la clientela più "vulnerabile", a causa di problemi o disservizi, per proporre quindi il cambio del proprio operatore telefonico.

TANTO A ME NON CAPITA

26 GIUGNO
FURTO DI INFORMAZIONI TIM

15 GIUGNO
GEOX PARALIZZATA

il mattino di Padova

Geox sotto attacco informatico: azienda paralizzata con richiesta di riscatto

FABIO POLONI

15 GIUGNO 2020

Montebelluna, i lavoratori della logistica del colosso trevigiano a casa per due giorni. I manager: «Task force al lavoro, soluzione nelle prossime ore»

Geox letteralmente ostaggio dei pirati informatici. Un attacco digitale sta tenendo sotto scacco il colosso trevigiano delle calzature, e gli hacker hanno chiesto un riscatto per togliere le catene virtuali (ma dagli effetti reali, e pesantissimi) che da ieri paralizzano l'azienda con quartier generale a Montebelluna. È già partita una denuncia alla polizia postale.

TANTO A ME NON CAPITA

26 GIUGNO
FURTO DI INFORMAZIONI TIM

15 GIUGNO
GEOX PARALIZZATA

8 GIUGNO
ENEL E HONDA

Ekans ransomware colpisce Enel e Honda, ecco come e gli effetti

Home > Malware e attacchi hacker > Ransomware

Condividi questo articolo

L'attacco è avvenuto tra il 7 e l'8 giugno, le due aziende confermano. Honda riporta qualche danno alla produzione in Europa. Enel parla di possibili disservizi, per un periodo di tempo limitato, alle attività di customer care. Ecco come funziona la nuova minaccia, il ransomware Ekans

09 Giu 2020

CYBERSECURITY360

TANTO A ME NON CAPITA

26 GIUGNO
FURTO DI INFORMAZIONI TIM

15 GIUGNO
GEOX PARALIZZATA

8 GIUGNO
ENEL E HONDA

30 MAGGIO
FALSO SITO GEOX

Truffe online, il falso sito Geox che promette sconti sulle scarpe

La Polizia di Stato, sul proprio sito, mette in guardia dall'ennesimo caso di truffa e fornisce un decalogo per non cascarci

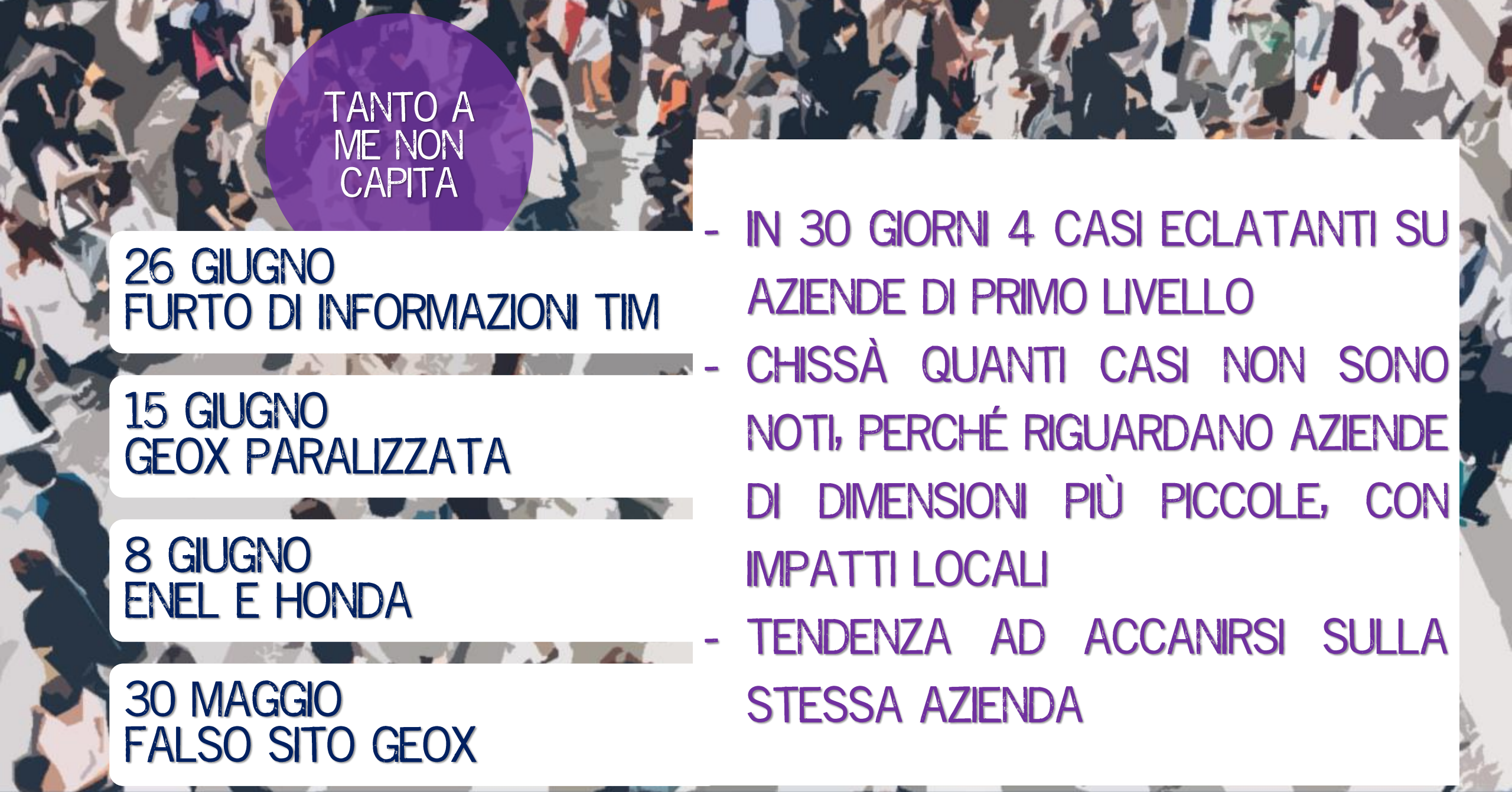
30 Maggio 2020

Condividi su Facebook +

Truffe, quali sono le telefonate più pericolose a cui non rispondere

Ai diversi tentativi di truffa ai danni di consumatori e naviganti del web, nelle ultime ore se ne è aggiunto un ennesimo. Se giorni fa girava su chat e social network un falso buono Ikea che però, con l'azienda svedese, non aveva nulla a che fare, questa volta il brand sfruttato dai truffatori per attirare i malcapitati è un celebre marchio di scarpe e abbigliamento: **Geox**.

il "sito truffaldino" geoxoutlet.online, che nelle ultime ore non risulta più raggiungibile, utilizzava logo e informazioni simili a quelli pubblicati sul sito ufficiale dell'azienda, con un dominio che può trarre in inganno.
Ancora una volta, l'obiettivo era quello di indurre gli utenti a fare acquisti via web, inserendo i dati della propria carta di credito, con la promessa di poter usufruire di forti sconti sui prodotti. La stessa società, però, ha messo in allerta i propri clienti, confermando che si tratta di un sito del tutto falso e di un'iniziativa in nessun modo collegata all'azienda.



TANTO A ME NON CAPITA

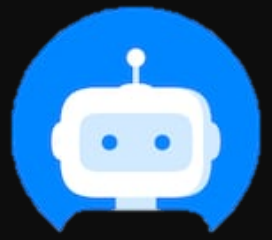
26 GIUGNO
FURTO DI INFORMAZIONI TIM

15 GIUGNO
GEOX PARALIZZATA

8 GIUGNO
ENEL E HONDA

30 MAGGIO
FALSO SITO GEOX

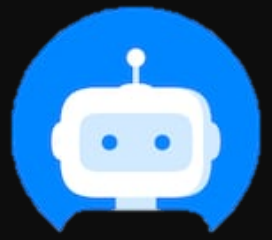
- IN 30 GIORNI 4 CASI ECLATANTI SU AZIENDE DI PRIMO LIVELLO
- CHISSÀ QUANTI CASI NON SONO NOTI, PERCHÉ RIGUARDANO AZIENDE DI DIMENSIONI PIÙ PICCOLE, CON IMPATTI LOCALI
- TENDENZA AD ACCANIRSI SULLA STESSA AZIENDA



Cyber security

Equipe specializzata e strumenti avanzati

Probabilità	Prevenire
Impatto	Curare



Cyber security

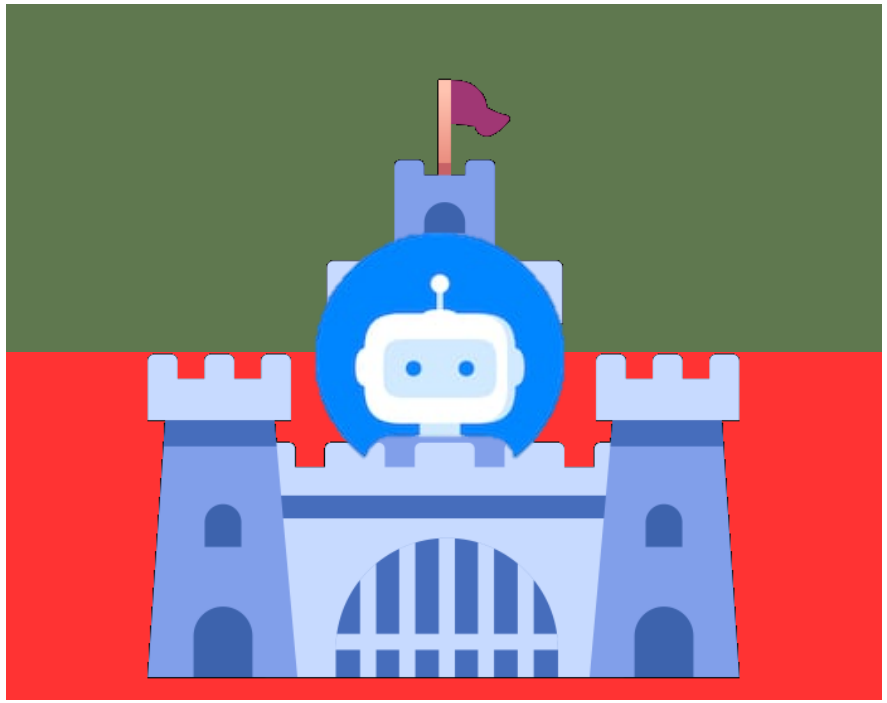
Equipe specializzata e strumenti avanzati

- Soluzioni anti-exploit e EDR (Endpoint Detection and Response) per tutti gli endpoint
- Soluzioni di controllo dell'accesso al network e autenticazione a due fattori
- Sistema di Network Access Control per ispezionare e bloccare i dispositivi non sicuri
- Usare le soluzioni CDR (Content Disarm and Recovery) per disattivare allegati malevoli
- Soluzione Cloud Access Security Broker (CASB) al posto di varie soluzioni SaaS non autorizzate.

- Segmentazione della rete in zone di sicurezza per prevenire la diffusione di attacchi e minacce
- Gestione del recupero dal ransomware nel piano di Business Continuity e Disaster Recovery
- Riduzione al massimo dei privilegi per gli utenti in modo che non possano infettare applicazioni, dati o servizi critici.
- Analisi con strumenti avanzati della provenienza di un'infezione e della effettiva rimozione.
- Raccolta rapida e continua delle informazioni sulle minacce e sugli attacchi attivi sulle reti, per fermare un attacco avanzato e combinati.

Cyber security

Un castello a protezione dell'azienda



Il dipendente

Ovvero come vanificare il castello

Hanno bloccato Youtube

Naviga usando il telefono come hot spot

Come si entra nel portale?

Ti mando la mia password, prova con quella

Il dipendente

Ovvero come vanificare il castello

Non trovo la relazione nel documentale

È nella pennetta, ora te la porto

Non riesco a mandarti l'allegato

Mandamelo su Gmail

Il dipendente

Ovvero come vanificare il castello

Il dipendente

Ovvero come vanificare il castello

Security Awareness

Innalzare il livello di sicurezza dell'organizzazione e l'efficacia dei sistemi di protezione dei dati attraverso la sensibilizzazione sulla sicurezza delle informazioni e sui corretti comportamenti.

Cyber security e Security awareness

Due facce della stessa medaglia