Dal Panico al Piano: Strategie immediate per rispondere ad un incidente Cyber

Matteo Cecchini – CEO T-Consulting Srl

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

Per una volta non parleremo di:

- Framework di Cybersecurity
- Metodologie di protezione
- Movimenti laterali
- EDR/XDR/SOC e altre «buzz»

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

Vedremo invece….

- Quanto a volte siamo noi stessi a rendere semplice il lavoro ad un attaccante
- Cosa fare DOPO che un attacco è avvenuto

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

Facilità di identificazione degli asset violabili – Esempio 1

SHODAN | Explore | Downloads | Pricing | country:it port:3389 city:"cesena"

TOTAL RESULTS
191

TOP ORGANIZATIONS

Telecom Italia S.p.A.	58
Telecom Italia S.p.A. TIN EASY LITE	28
[redacted] srl	27
[redacted] S.p.A.	19
Vodafone Italia S.p.A.	8

More...

TOP PRODUCTS

Remote Desktop Protocol	186
VNC	1
nginx	1

TOP OPERATING SYSTEMS

Windows (build 10.0.19041)	49
Windows (build 10.0.17763)	36
Windows 11 (version 22H2) (build 10.0.22621)	35
Windows (build 10.0.14393)	15
Windows 7 Professional	5

More...

View Report | Download Results | Historical Trend | Browse Images | View on Map | Advanced Search

Partner Spotlight: Looking for a Splunk alternative to store all the Shodan data? Check out Gravwell

185.94[redacted]
Latosec srl
Italy, Cesena
self-signed

SSL Certificate
Issued By:
|- Common Name: [redacted].it
Issued To:
|- Common Name: [redacted].it
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

2024-11-01T14

Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
OS: Windows 10 (version 1809)/Windows Server 2019 (version 1809)
OS Build: 10.0.17763
Target Name: TERMINAL
NetBIOS Domain Name: TERMINAL
NetBIOS Computer...

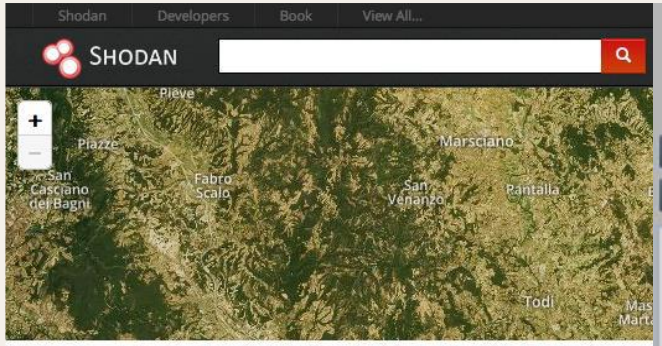
95.255[redacted]
Telecom Italia S.p.A.
Italy, Cesena
self-signed

SSL Certificate
Issued By:
|- Common Name: HPE1
Issued To:
|- Common Name: HPE1
Supported SSL Versions:
TLSv1, TLSv1.1, TLSv1.2

2024-11-01T14

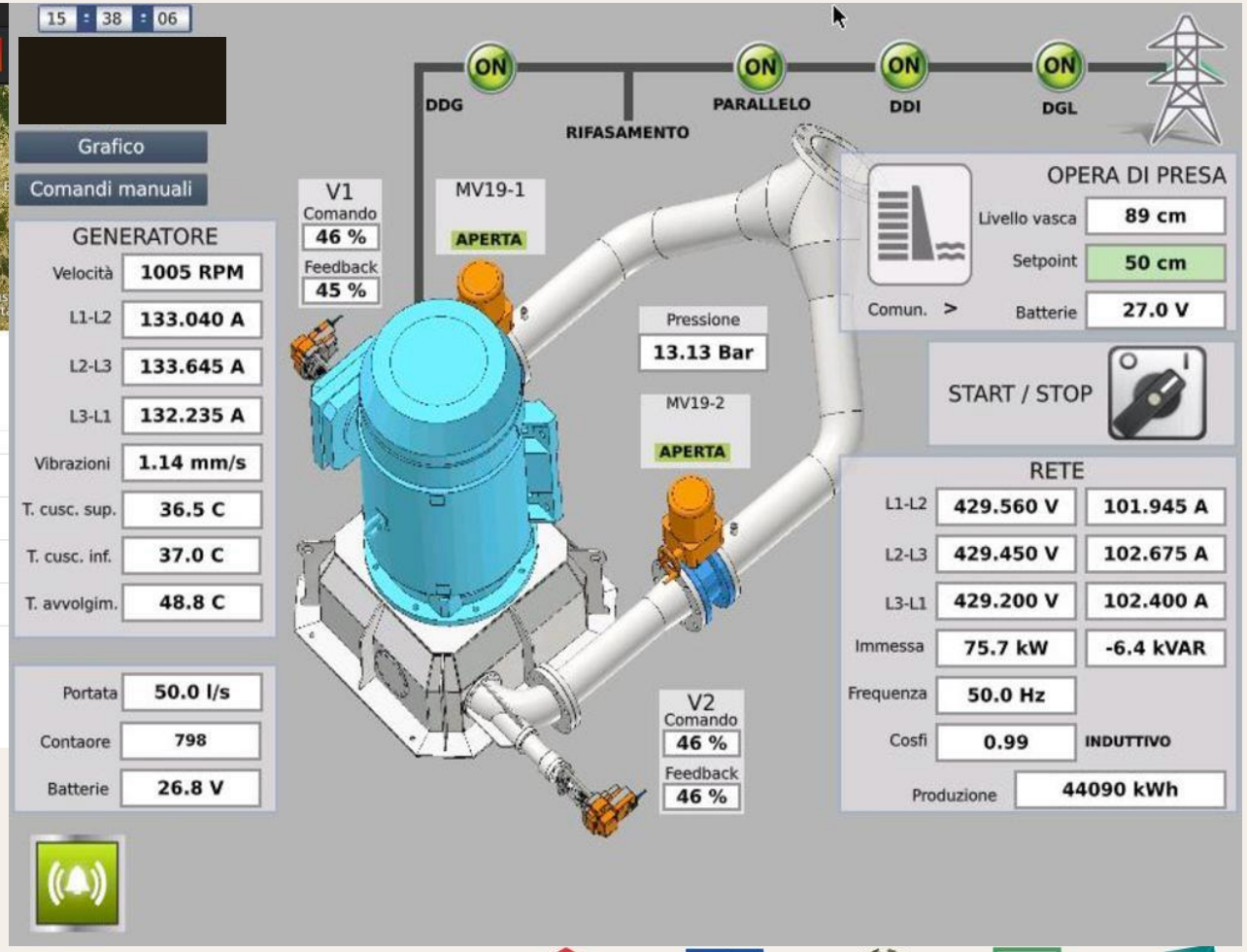
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
OS: Windows Server 2022
OS Build: 10.0.20348
Target Name: HPE1
NetBIOS Domain Name: HPE1
NetBIOS Computer Name: HPE1
DNS Domain Name: HPE1
FQDN: HPE1
...

Facilità di identificazione degli asset violabili – Esempio 2



88.147.[redacted]

Country	Italy
Organization	[redacted]
ISP	[redacted]
Last Update	2016-04-11T13:38:55.074548
ASN	AS29096

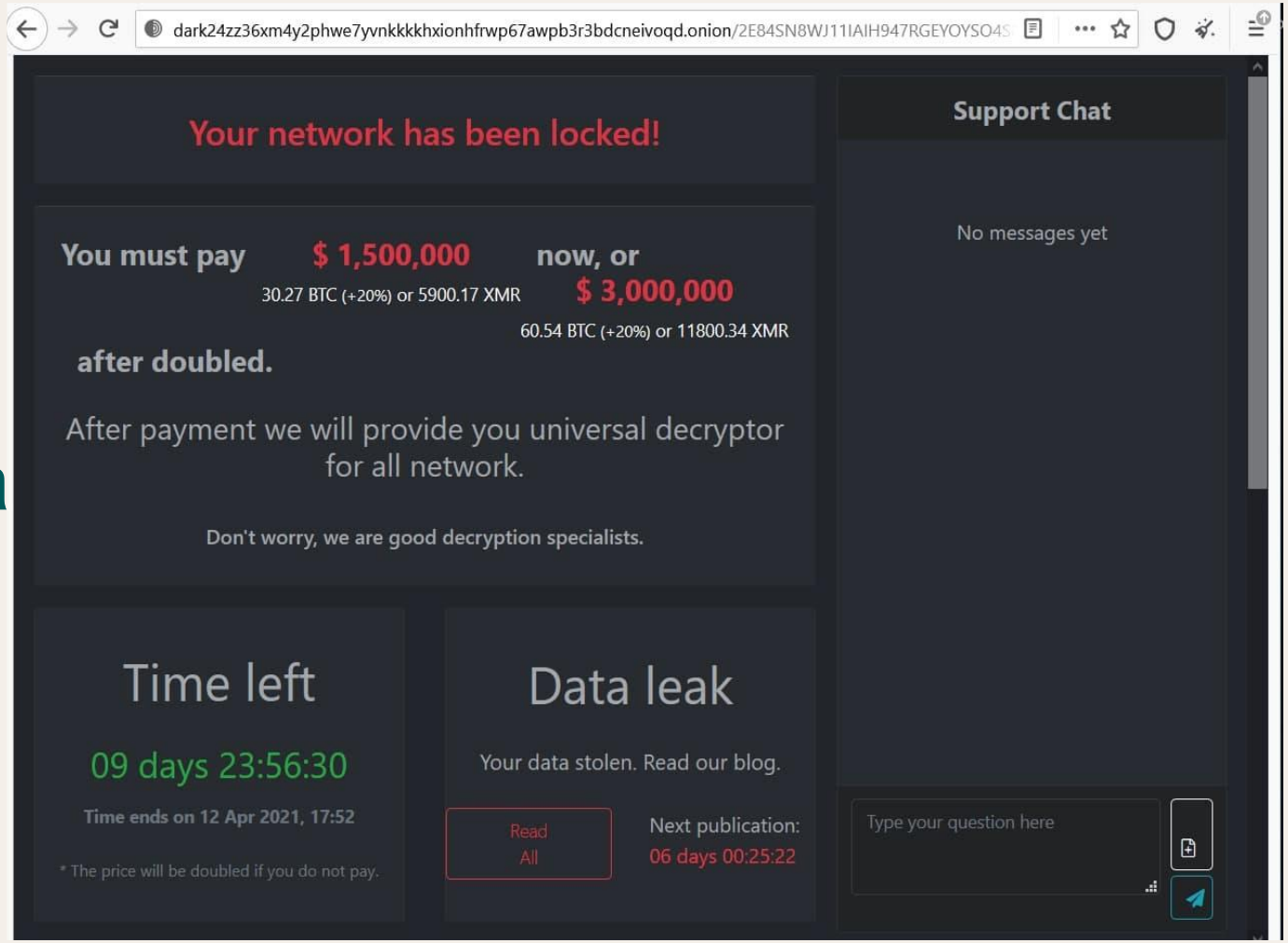


Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

E così un lunedì mattina…

Riscatto con doppia estorsione

- Distruzione dei dati cifra sui sistemi aziendali
- Pubblicazione dei dati sottratti



Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

Panico

E adesso?

Prima di tutto occorre ricordarsi alcune regole auree:

- Il tempo gioca a nostro **sfavore**
- Improvvisare non è una strategia (ricordate bene questa frase)
- Il processo di risposta ad un incidente Cyber non è né semplice né breve
- La trasparenza, paga. Sempre.
- Soprattutto quando si parla di comunicazione!!

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

STEP 1 – Contenimento e raccolta delle informazioni

- Occorre limitare la capacità operativa di chi ha attaccato
  - Isolare i sistemi compromessi gli uni dagli altri (se la minaccia lo consente)
  - Scollegare l'infrastruttura da Internet
- Raccogliere informazioni
  - Comprendere il perimetro dell'attacco
    - Quali sistemi sono compromessi?
    - I backup sono disponibili?
  - Mettere al sicuro le evidenze dell'attacco
    - Mettere al sicuro i Log dei sistemi compromessi e dei sistemi critici (anche se non compromessi!)

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

STEP 2 – Eradicazione della minaccia

- Identifico la minaccia e la elimino
  - Ransomware: attenzione a verificare che non vi siano più copie sparse per la rete
  - Esfiltrazione di dati:
    - Occorre identificare i canali utilizzati per il furto dei dati e renderli inerti
    - Dobbiamo capire quali dati sono stati trafugati (Data Breach?)

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

STEP 3 – Ripristino

- Due possibilità
  - Recupero dai backup (nel caso sia tutto crittografato)
  - Pulizia e hardering dei sistemi (scelta rischiosa)
- E' una fase molto delicata perché:
  - Spesso la prima cosa che fanno gli attaccanti in caso di ransomware è compromettere i backup
  - Se non ho i backup…. ho un problema.
  - Se non ho i backup…. le (eventuali) soluzioni potrebbero essere estremamente dispendiose.
- Quindi…
  - Regola del 3-2-1-1
  - I backup non bastano -> serve il Disaster Recovery

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

STEP 4 – Analisi Post Incidente

- Ok, siamo riusciti ad uscirne…e adesso?
  - Fermarsi e analizzare cosa ha portato all'incidente
    - Da dove sono entrati? Come hanno fatto?
    - Le mie misure di sicurezza dove hanno fallito?
    - Ho un problema con la consapevolezza degli utenti rispetto alle minacce Cyber?
  - Evitare che ricapiti qualcosa di simile ma soprattutto:

PREPARARE UN PIANO DI INCIDENT RESPONSE

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.

Domande da porsi, PRIMA di un attacco

- Quanto incide la perdita dei dati sulle mie entrate o sui costi?
- Se dovessi riacquisire i dati persi, quanto mi costerebbe?
- Quanto costerebbe all'azienda la perdita dei dati a seguito di un attacco informatico?

MENU | CERCA la Repubblica ABBONATI | QUOTIDIANO R | ACCEDI

HOME CRONACA QUARTIERI SPORT FOTO RISTORANTI VIDEO ANNUNCI LOCALI CAMBIA EDIZIONE

adv

ERT / Teatro Nazionale
Direzione Valter Malosti
Stagione 21/22

Arena del Sole

Campagna abbonamenti
dal 14 settembre

051 2910910
bologna.emiliaromagnateatro.com

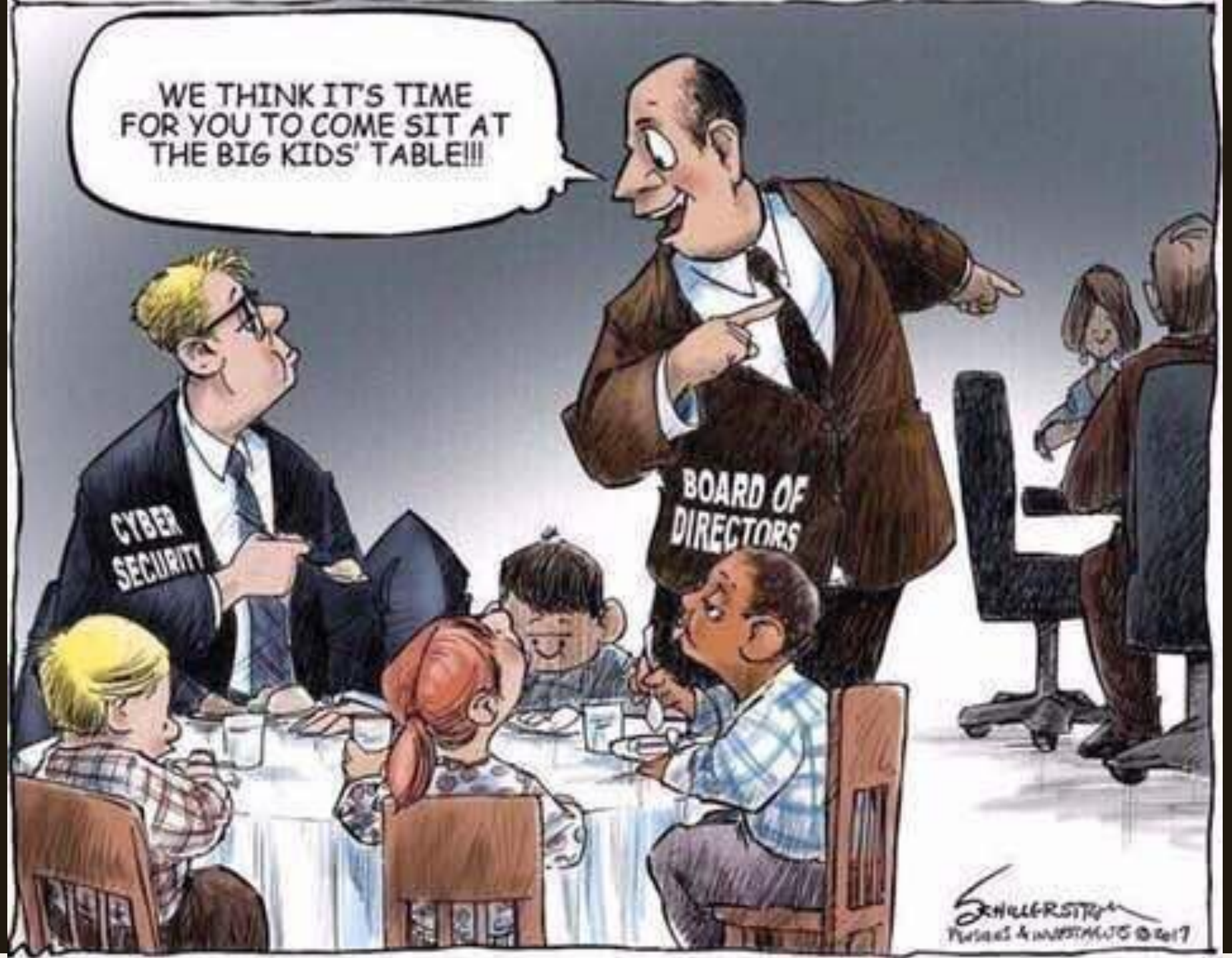
R CONTENUTO PER GLI ABBONATI

Vintag, un misterioso crash dei server cancella i dati degli utenti: addio alla stella nascente delle app del vintage

di Marco Bettazzi

Sulla start up bolognese avevano investito fondi stranieri e anche l'azienda Piquadro. L'ad: "Costretti a chiudere ma faremo causa"

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.


WE THINK IT'S TIME FOR YOU TO COME SIT AT THE BIG KIDS' TABLE!!!
CYBER SECURITY
BOARD OF DIRECTORS

Grazie dell'attenzione

m.cecchini@t-consulting.it

Il progetto Romagna Tech Digital Team è realizzato grazie ai Fondi europei della Regione Emilia-Romagna.