DIGIMETRICA

GEOPOLITICA E MINACCIA CIBERNETICA: UN VIATICO PER ISTITUZIONI E AZIENDE

Pescara, 26 maggio 2022

I MAGGIORI RISCHI GEOPOLITICI

- Impatto del Covid-19
- Aumento della rivalità di potere
- Localismo contro globalismo
- Multinazionali a rischio
- Terrorismo e conflitti armati
- Cyber e corsa alla tecnologia: rischio del decoupling tecnologico Cina/USA
- Malcontento sociale e conflitti locali
- Cambiamento politico

COME LE GEOPOLITICA SPINGE LA MINACCIA CIBERNETICA

I RISCHI CYBER

Fino al 2015, i rischi “cyber” non erano nemmeno considerati all’interno del Global Risk Report del World Economic Forum.

Già dal 2019 sono assurti al primo posto per impatto e probabilità di accadimento, insieme ai disastri naturali ed agli effetti globali del climate change.

Sono problematiche che:

- per natura, gravità e dimensione travalicano costantemente i confini dell’ICT e della stessa Cyber Security;
- hanno impatti profondi, duraturi e sistemici su ogni aspetto della società, della politica, dell’economia e della geopolitica .

Perdite stimate:

- 1 trilione di dollari per il 2020;
- 6 trilioni per il 2021.

Emergenza globale, concreta, un “clear and present danger” che incide ormai per una percentuale significativa del prodotto lordo mondiale.

I TREND:

- Organizzazioni hacker sempre più potenti;
- sicurezza del e nel Cloud;
- Intelligenza Artificiale: è possibile che le cybergang utilizzino AI «antagoniste»;
- sicurezza della Supply Chain;
- IoT e Industria 4.0.;
- «certificazioni» sempre più importanti;
- gli attacchi ransomware servono motivi «ibridi»;
- le sempre maggiori interrelazioni tra safety e security che la digitalizzazione comporta, rendendone più labili i confini, segnalano la necessità di un approccio «olistico» alla sicurezza.

CRIMINALITÀ INFORMATICA OGGI

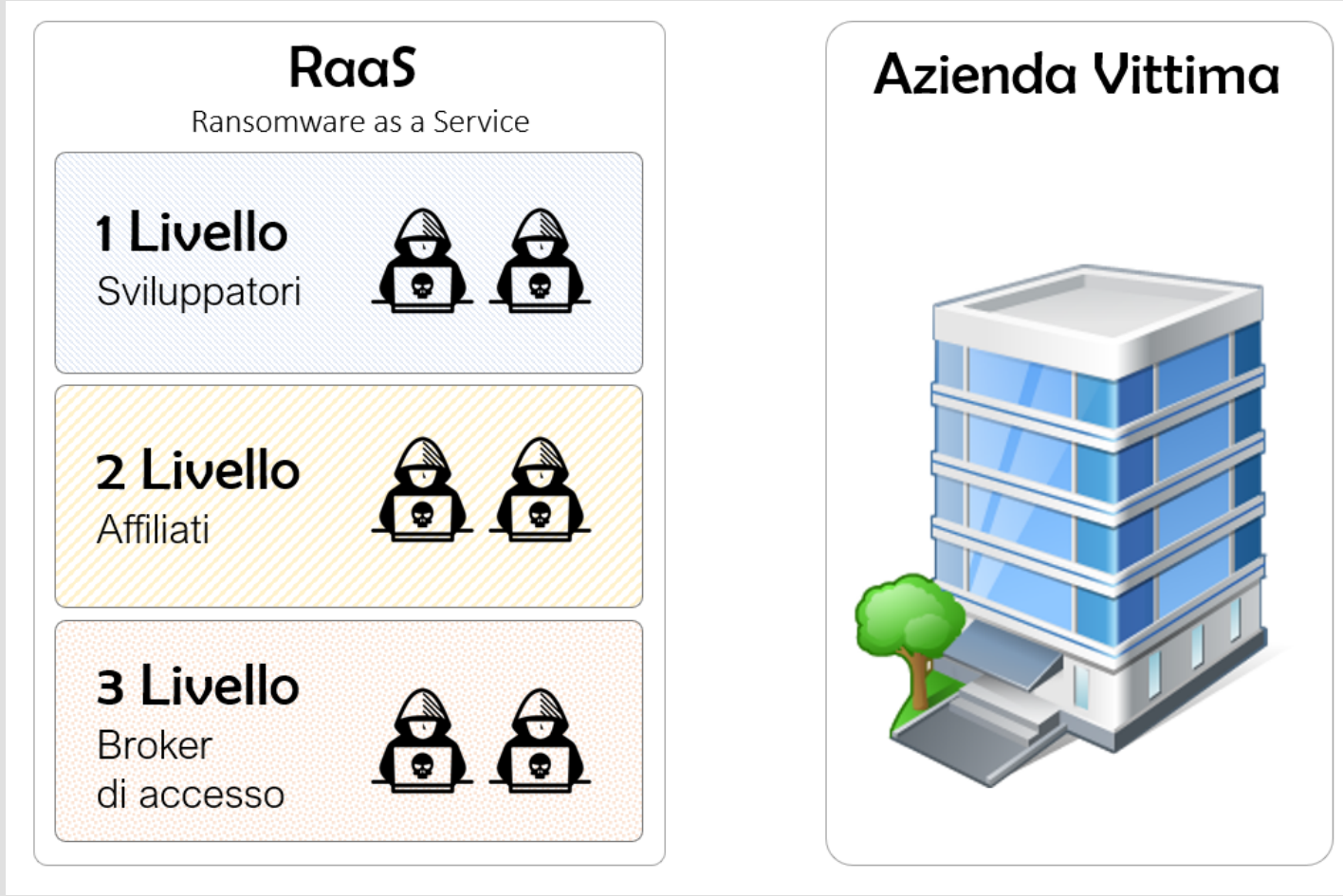
L'idea «romantica» dell'hacker che «smanetta» in soffitta: tramontata.

Cybergang:

- Investono nella ricerca di nuove vulnerabilità nei software legali da usare come «breccia» per introdursi nei sistemi IT target;
- usano il modello di «Hacking-as-a service», «Ransowmare as a Service» e «Disinformation-as-a-Service»: anziché condurre azioni in proprio, vendono l'uso degli strumenti di attacco ad altri gruppi, per aumentare la penetrazione e ridurre i rischi;
- conducono campagne di attacco e disinformazione per conto degli

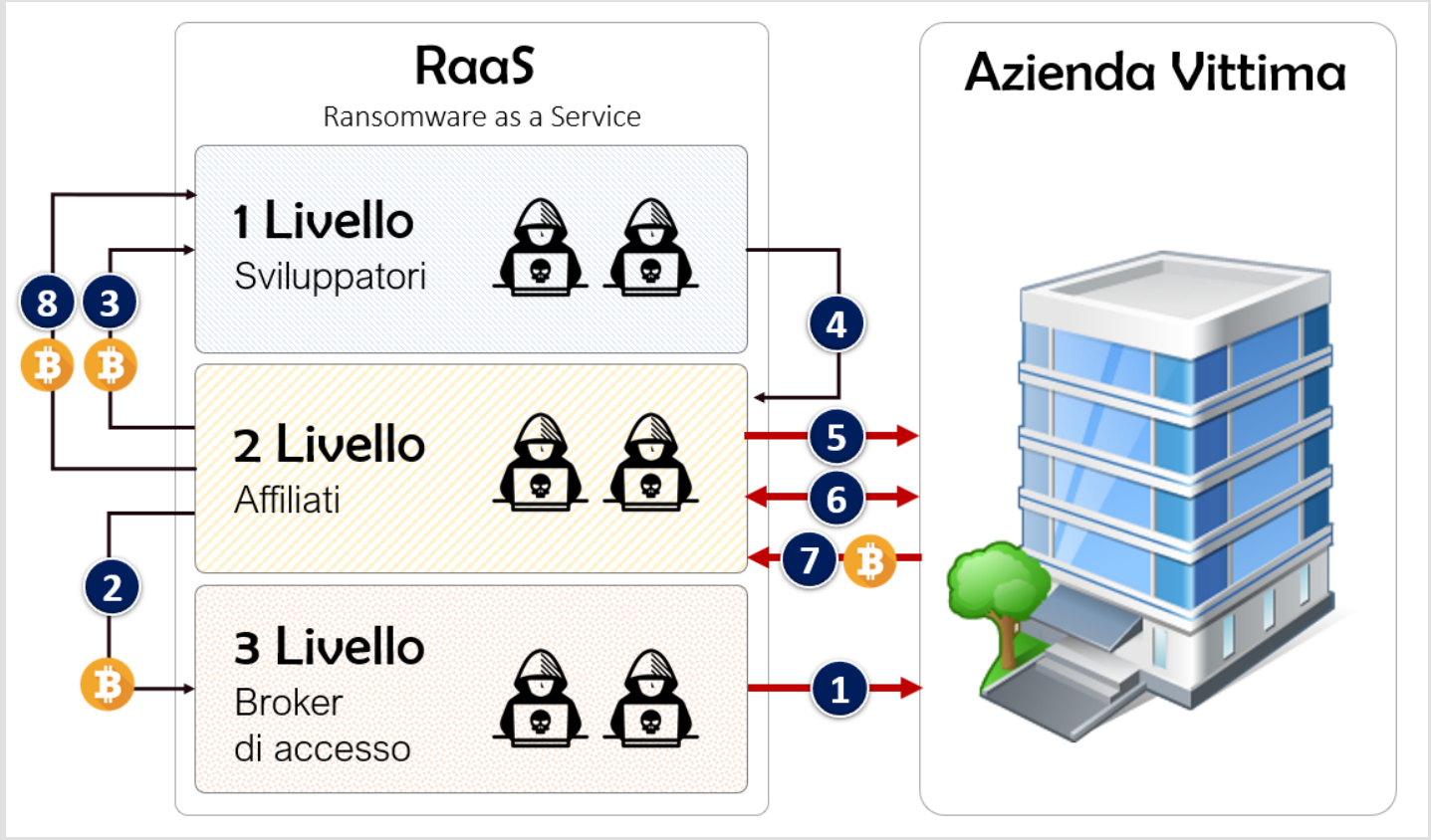
ORGANIZZAZIONE DEL RAAS

(Fonte: RedHotCyber - Massimiliano Brolli & Serena Carlini)



MODELLO OPERATIVO DEL RAAS

(Fonte: RedHotCyber - Massimiliano Brolli & Serena Carlini)



Sicurezza della Supply Chain

I fornitori si integrano con i processi e le infrastrutture IT delle aziende clienti o «capo filiera».

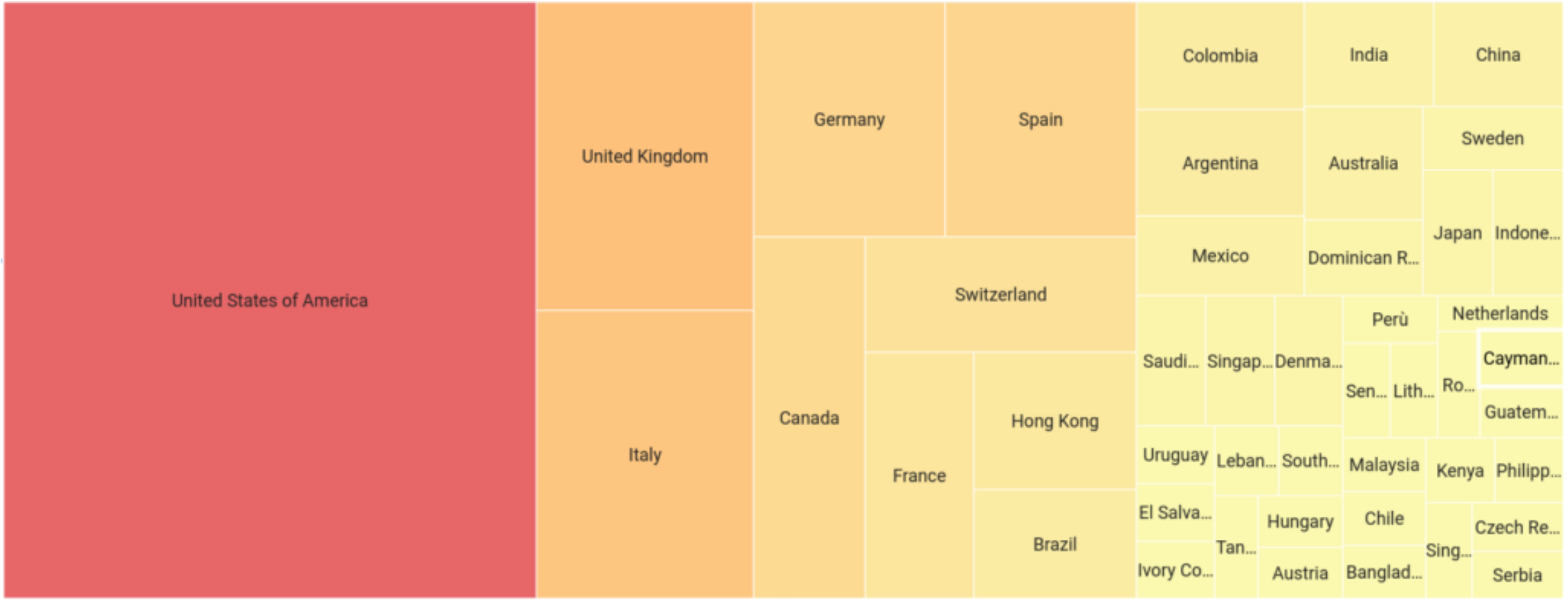
Gli investimenti in cybersecurity rendono le aziende «capo-filiera» meno permeabili.

Vengono prese di mira le catene di fornitori, che presentano misure di sicurezza meno robuste o addirittura inesistenti

Ponemon Institute: nel 2021 gli attacchi di terze parti hanno rappresentato il 42% di tutti i casi.

NAZIONI PIÙ COLPITE DA ATTACCHI RANSOMWARE A MARZO 2022

(Fonte: Ransomware Data Room)



RICORDIAMO ALCUNI PUNTI FONDAMENTALI

La sicurezza informatica viene, erroneamente, considerata troppo spesso una materia altamente tecnica, comprensibile quindi solo da esperti informatici.

Tuttavia, sul piano operativo, non basta «buon senso» e «logica» o, al massimo, qualche misura di prevenzione: occorrono specialisti

Infatti non ci si può difendere «da soli», a meno che non si disponga di risorse adeguate e personale specializzato.

Perché violare una qualsiasi organizzazione oggi dipende da motivazione, tempo e skill

- Se un gruppo hacker è ben finanziato, motivato ed ha forti competenze tecniche oltre che tempo, le possibilità che i suoi attacchi abbiano successo sono elevate; se le infrastrutture informatiche fossero sicure, procederà con l'ingegneria sociale e se anche questa strada risultasse poco percorribile, cercherà un insider; pertanto colpirà in primo luogo il livello tecnologico per poi passare, ove questo non basti, al livello più nevralgico e poco controllabile per sua natura, il livello umano.

PERCHÉ SIAMO AL TERZO POSTO

Regola base: violare le aziende che permettono il massimo ritorno economico, utilizzando il minor tempo possibile.

01

Purtroppo, le infrastrutture delle organizzazioni sia pubbliche che private, risultano poco dispendiose da violare e le richieste di riscatto vengono assecondate (si vede nelle blockchain).

02

Non si fa «lesson learned»: non si divulgano i «vettori di attacco» (partendo dai propri errori), per non infangare la propria web & brand reputation.

03

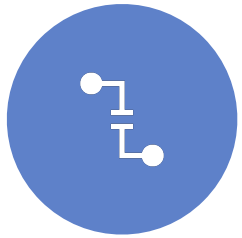
Mancano quindi condivisione, collaborazione, rete e divulgazione.

COSA DOVREBBERO FARE LE IMPRESE

EFFETTUARE UNA SERIA ANALISI DI QUANTO E COME IL SISTEMA INFORMATIVO AZIENDALE SIA ESPOSTO A RISCHIO.

DISPORRE DI UNA SERIE DI MISURE LOGICO-ORGANIZZATIVE CHE POSSANO RENDERE MENO VULNERABILI L'ORGANIZZAZIONE E LE PROCEDURE DI UN'AZIENDA.

FORMAZIONE: SVILUPPARE LA CULTURA DELLA "CYBER SECURITY".



UTILIZZARE SECURITY INTELLIGENCE.

AFFIDARSI A PROFESSIONISTI DELLA SICUREZZA.

CHE SUCCEDE OGGI

Guerra in Ucraina: non c'è stato ancora nessun vero attacco informatico.

Pretesto Eurovision Song Contest.

Gli attacchi DDoS a cui stiamo assistendo sembrerebbero essere solo le prime avvisaglie di attività molto più pesanti e invasive.

COS'HA INSEGNATO FINORA LA GUERRA IN UCRAINA

- Uno dei grandi vantaggi degli attacchi informatici è la difficolta di attribuire l'attacco stesso
- Questa caratteristica può essere fondamentale in una guerra a lungo termine e a bassa intensità.
- I grandi attacchi informatici richiedono però una lunga ed accurata preparazione per raccogliere informazioni, programmare gli exploit e quant'altro.
- Una volta avviata una guerra di conquista, gli strumenti militari convenzionali appaiono più efficienti al fine.
- Quello ucraino è l'esempio di come convenga investire

TUTTO RESTERÀ COSÌ?

- Secondo David Duncan, direttore della società di sicurezza Redpoint Labs (New York), le cybergang russe si concentreranno sulle società occidentali, specie quelle dei paesi NATO che supportano l'Ucraina.

- Questo potrebbe risultare particolarmente vero qualora la Russia dichiarasse conclusa la campagna militare con l'occupazione dell'intero Donbass, aprendo ad un periodo di tregua armata.

Lezione

La cyber security è tanto più efficace quanto più è diffusa e condivisa.

È uno dei leit motiv della nuova Strategia Nazionale di cybersicurezza.

Istituzione della Agenzia per la cybersicurezza nazionale (d.l. 14 82/2021).

Strategia Nazionale di Cybersicurezza – Sfide da affrontare

Assicurare una transizione digitale cyber resiliente della Pubblica Aministrazione (PA) e del tessuto produttivo.

Autonomia strategica nazionale ed europea nel settore del digitale.

Anticipare l'evoluzione della minaccia cyber.

Gestione di crisi cibernetiche.

Contrastare la disinformazione online nel più ampio contesto della cd. minaccia ibrida.

Formazione

Strategia Nazionale di Cybersicurezza – La riorganizzazione dell'architettura nazionale di cybersicurezza alla luce del d.l. 82/2021

Strategia Nazionale di Cybersicurezza – fondi disponibili

- Fondi nazionali: quota percentuale (1,2%) degli investimenti nazionali lordi su base annuale.
- Finanziamenti provenienti dai programmi Orizzonte Europa ed Europa digitale.
- Art. 6 del Regolamento (UE) 2021/887 del 20 maggio 2021: i finanziamenti vengono convogliati dal Centro europeo di competenza per la cibersicurezza (ECCC), alla Rete dei Centri Nazionali di Coordinamento (NCC), di cui ACN è parte.
- PNRR, misura 1.5 “Cybersecurity”: investimento pari a 623 mln €, rimesso all’ACN soggetto attuatore.

Strategia Nazionale di Cybersicurezza- obiettivi da perseguire

Strategia Nazionale di Cybersicurezza – architettura nazionale per la gestione degli incidenti e delle crisi di cybersicurezza

La ACN fa parte della rete CyCLONe (Cyber Crisis Liaison Organisation Network) e della rete europea degli CSIRT.
In particolare, la rete CyCLONe, per la risposta rapida alle crisi e agli incidenti cyber transfrontalieri su larga scala, mira, tra l'altro, a raccordare il livello politico europeo - Consiglio UE, anche tramite i meccanismi integrati per la risposta politica alla crisi (Integrated Political Crisis Response - IPCR) - con il livello tecnico, ovvero gli CSIRT nazionali e la rete europea degli CSIRT.

Digital Europe Programme:

- aiuterà l'UE a raggiungere un livello comune elevato di cybersicureza;
- offre la possibilità di rafforzare il livello comune di cybersicurezza in tutta l’UE;
- è un programma di investimento che aiuta l'UE a realizzare un quadro basato sui valori per la tecnologia;
- include il GDPR, la nuova direttiva sulla sicurezza delle reti e dei sistemi informativi (NIS2), l'intelligenza artificiale e le disposizioni sui servizi e sui mercati digitali.

DIGIMETRICA

GRAZIE PER L'ATTENZIONE

WWW.DIGIMETRICA.COM