IT•NEWS

N. 6 MAR./APR. 2022

L'indispensabile road-book

per rendere sempre più digitale e competitiva la tua impresa

IN QUESTO NUMERO

L'EDITORIALE

A cura di **Alessio Angioli**

Metaverso la rivoluzione del futuro di internet

oppure si prospetta una grande bolla virtuale?

Se ne fa un gran parlare, Metaverso è sulla bocca di tutti ma quanto ne sappiamo veramente? Non tutti hanno le idee chiare, perché fino ad oggi era un concetto impensabile.

Da quando Zuckerberg ha chiamato la holding del gruppo "Meta" (che controlla Facebook, Instangram, Whatsapp e gli Oculos), il fenomeno del **Metaverso** è esploso promettendo mondi virtuali in cui tutti contiamo di acquistare o usufruire virtualmente di qualcosa. Si prospettano degli spostamenti ed interessi molto forti, soprattutto economici, dal mondo reale a quello dei nostri device.

I "Metaversi" sono mondi paralleli, realtà virtuali simili a quelle dei videogiochi come the Sims, Fortnite o Roblox. Gli utenti tramite i loro avatar potranno interagire tra loro, stringere rapporti e relazioni, oppure teletrasportarsi come ologrammi in ufficio o ad un concerto. L'universo del mondo reale e quello digitale si uniscono, si possono fare acquisti di vario tipo come isole e altre proprietà digitali.

Grazie agli NFT, il possesso dei beni digitali è certificato, l'acquisto avviene utilizzando monete virtuali che si ottengono con denaro reale. Ogni settore riceverà richieste che alimenteranno il nuovo mercato, i costi della produzione verranno azzerati mentre gli introiti diverranno immensi. O almeno è questo che ci si aspetta.

Su Metaverso, hanno puntato e investito vari Brand delle Grandi Firme, che stanno già iniziando a lanciare le proprie collezioni virtuali, aumentando la realtà con l'utilizzo di visori VR e occhiali smart 3d. Un pianeta che intende offrire in una formula ancora più universale rispetto a quella che già conosciamo, la possibilità di raccontare ed esportare il proprio sistema valoriale, il proprio branding e i propri prodotti avvicinandosi sempre di più a quello che sarà il pubblico del futuro, ovvero la generazione Z.

Non è sbagliato creare nuovi punti di contatto, provare anche a capirsi un po' di più e creare nuovi ponti verso il futuro, ma quali rischi si corrono? L'evoluzione del cyberspazio genererà nuovi modelli di business spostando l'economia reale a quella virtuale, con il rischio di far scoppiare una bolla. Per gli utenti, potrebbe essere alto il rischio di esposizione al monitoraggio costante o di compromissione della sicurezza dei dati.

I più avanguardisti sostengono che un giorno, neanche troppo lontano, la virtualizzazione sarà onnipresente e inevitabile, perché facente parte di uno dei tanti passaggi generazionali. I più avvantaggiati sono sicuramente i giovani: per loro, avere una collezione digitale di qualcosa è naturale. Si tratta di un profondo mutamento in cui si rinnova il concetto d'identità: l'experience immersiva nel Metaverso creerà il medesimo ecosistema emozionale come se fossimo fisicamente presenti. L'esperienza fisica e virtuale andranno completandosi, si parlerà di interattività e di esperienza omnichannel.

L'interoperabilità fra mondi e piattaforme è una delle grandi scommesse di Metaverso e secondo gli analisti di Bloomber Intelligence l'opportunità di mercato è stimata per un valore di 800 miliardi di dollari entro il 2024.

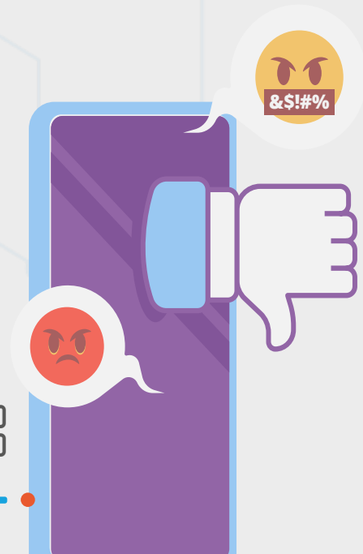
Cosa ci riserverà il Metaverso? Lo scopriremo nel tempo

LA SICUREZZA A 360°

IT SECURITY

A cura di
Marco Melucci

CYBERBULLISMO



La **generazione Z** è fortemente dipendente dalle tecnologie e da internet a tal punto da distinguere con difficoltà la realtà fisica da quella virtuale. Il **cyberbullo** tormenta le sue vittime online, senza dare tregua, attraverso la strumentalizzazione dei social o delle App che contengono messaggistica e chat. In questi casi, la tecnologia digitale, può causare pressioni enormi sulle vittime, danni irreparabili se i ragazzi vengono abbandonati a sé stessi. In passato i bulli erano soliti perseguitare i compagni di classe e i ragazzi più deboli che avevano a tiro. Chiaramente, le molestie non facevano meno male, ma quantomeno venivano interrotte con la distanza.
Oggi, le vittime sono perseguitate prima a scuola e poi online impattando sulla loro esistenza a 360 gradi.
La vittima, non è detto sappia chi ci sia veramente dall'altra parte, le minacce potrebbero provenire da qualsiasi parte del mondo. Tutti possono essere esposti, ma i più giovani sono maggiormente alla mercé di questa tipologia di pericolo. Questo fenomeno si sta espandendo molto velocemente e non è facile debellarlo, proprio perché la tecnologia è sempre più parte integrante della nostra vita. La tecnologia non è da demonizzare, ci avvantaggia nella vita di tutti giorni, dobbiamo solo imparare a gestire alcune problematiche che dipendono dall'errore umano.
Per questo, dal 2017 in Italia è entrata in vigore la legge 71 che tutela le vittime di cyber bullismo, in cui si prevede un **maggiore controllo del web** e un **maggiore coinvolgimento nelle scuole**. Il minore e i genitori hanno diritto a richiedere l'oscuramento del materiale che li riguarda con rimozione del contenuto entro 48 ore. La scuola è tenuta ad assegnare ad un professore il ruolo di referente contro le iniziative di cyberbullismo. Inoltre, sono previste **iniziative in cui si sensibilizzano i ragazzi verso un utilizzo consapevole e sano di internet** in virtù di prevenzione contro il cyberbullismo. La tecnologia nel cyberbullismo è il vettore di questo nuovo fenomeno e allo stesso tempo è la soluzione al problema che, come un boomerang, torna indietro proteggendo i più deboli. Come? Sono state sviluppate APP basate su sistemi AI che tracciano contenuti di messaggi sospetti sugli smartphone dei ragazzi e sulle piattaforme dei social media, avvisando i genitori in tempo reale se il loro bambino viene minacciato. Viene riconosciuto l'atteggiamento degli utenti all'interno del testo, consentendo al sistema di rilevare in modo accurato il bullismo informatico.

<u>Una corretta cultura digitale rimane comunque la prima azione da intraprendere: educare i ragazzi sin da giovanissimi all'uso responsabile della rete e dei social, fare una distinzione netta tra reale e virtuale per limitare i rischi, per non cadere nelle trappole dei bulli.</u>

Gli I-TEAM promuovono la tecnologia ma sono contro i fenomeni che la sfruttano per danneggiare gli altri, fornendo un **servizio di rilevazione Cyberbullismo**.

NUOVE MANOVRE: novità bonus, incentivi e crediti di imposta

A cura di
Federico Melucci

Con la legge di bilancio 2022, il governo ha rifinanziato numerosi incentivi per sostenere le imprese. Dai crediti di imposta ai bonus, ecco gli strumenti finanziari più interessanti per le Pmi, secondo quanto comunica il Mise, con l'obiettivo di "sostenere" la competitività delle imprese stimolando gli investimenti in **INNOVAZIONE TECNOLOGICA**, ricerca e sviluppo, design e ideazione estetica.

BANDA ULTRALARGA:
APERTE LE RICHIESTE DEI VOUCHER

Il 15 Dicembre è arrivato il via libera della Commissione UE alla fase 2 del Piano voucher, per un totale di 610 milioni di Euro con il fine di sostenere l'accesso di piccole e medie imprese a connessioni internet veloci. Gli aiuti saranno destinati a quelle aziende che usufruiranno di servizi a banda larga in grado di garantire una velocità di download di almeno 30 megabit al secondo (Mbps).

L'obiettivo è quello di portare le aziende verso connessioni di maggiori capacità per renderle maggiormente efficienti e competitive nel sistema produttivo italiano.

I voucher favoriranno un maggiore utilizzo delle connessioni veloci da parte delle PMI:

- **abbonarsi a nuove connessioni**
- **potenziare le connessioni esistenti**
- **il bonus prevede la copertura di una parte dei costi di installazione dei servizi a banda larga ad alta velocità e del canone mensile**

Le imprese possono già richiedere fino ad esaurimento del fondo il Bonus Connettività **pari di 300 Euro, fino ad un massimo di 2.500 Euro** per incrementare la diffusione delle connessioni veloci in azienda.

Per inviare la richiesta seguire la procedura su **Infratel Italia**.

MENTRE DAL **21 FEBBRAIO VIA LIBERA** PER RICHIEDERE IL **SUPERBONUS TURISMO**

Sono arrivati i **contributi a fondo perduto per il turismo 2022**, erogati dall'agenzia Invitalia. Dal **21 febbraio**, data di attivazione della piattaforma online, i soggetti interessati potranno inviare la domanda. Il settore del turismo è stato colpito duramente dalla pandemia e proprio per questa ragione è necessario rivoluzionare il proprio business, anche se spaventa molto. **Ogni struttura ricettiva dovrebbe ripartire seguendo i trend dell'innovazione digitale e dei sistemi tech avanzati.**

COSA

Il provvedimento ritiene ammissibili le spese per i seguenti interventi di digitalizzazione:

- Impianti Wi-FI
- Siti Web ottimizzati per il sistema mobile
- Programmi per la vendita diretta di servizi e pernottamenti e la distribuzione sui canali digitali
- Spazi e pubblicità per la promozione e commercializzazione di servizi e pernottamenti turistici sui siti e piattaforme informatiche, anche gestite da tour operator e agenzie di viaggio
- Servizi di consulenza per la comunicazione e il marketing digitale
- Strumenti per la promozione digitale di proposte e offerte innovative in tema di inclusione e di ospitalità per persone con disabilità
- Servizi relativi alla formazione del titolare o del personale dipendente, collegata alle attività riportate nei punti precedenti.

CHI

I soggetti beneficiari:

- Imprese alberghiere
- Strutture che svolgono attività agrituristica
- Strutture ricettive all'aria aperta
- Imprese del comparto turistico, ricreativo e congressuale
- Stabilimenti balneari
- Complessi termali
- Porti turistici
- Parchi tematici compresi acquatici e faunistici

Il rilancio del settore turistico prevede la digitalizzazione dei propri servizi approcciandosi a tecnologie moderne; **verrà premiata l'Hospitality accessibile e sostenibile resa idonea da un'infrastruttura tecnologica che consenta di migliorare i servizi dei propri ospiti.**

IMPRENDITORI DEL SETTORE HOSPITALITY,
se volete superare le perdite del passato e affrontare le nuove sfide del mercato, contattate I-TEAM e richiedete preventivi per questa opportunità irripetibile.

INFORMAZIONI "LOGICHE"

IT SOFTWARE

A cura di
Marco Cecchi e Tommaso Alati

Il leggendario:
ESET ANTIVIRUS ENDPOINT SECURITY

I device sono i nostri compagni di lavoro, di viaggio e di casa, sono diventati sostanzialmente i nostri compagni di vita quotidiana. Grazie ai processi di trasmissione istantanei rappresentati dalle applicazioni, condividiamo, conserviamo e archiviamo un'enorme quantità di documenti e dati. Ci hanno fatto guadagnare tempo e denaro, ma i dati hanno suscitato molto interesse nei cyber criminali facendoli concentrare sulle modalità di azione per colpire le applicazioni.

Dietro richieste di riscatto o semplici esfiltrazioni dei dati ci sono spesso campagne di phishing e altre tattiche come il lancio di ransomware che puntano all'elemento più penetrabile della catena: l'essere umano. A subire moltissimi disagi ed infrastrutture bloccate per giorni, sono le aziende e le strutture sensibili perché vulnerabili a causa delle fragilità che riguardano la cyber security dell'intero sistema aziendale.

Uno degli Asset più importanti da mettere a budget per la vita della propria azienda è avere un **sofisticato sistema di protezione**. Non è un caso che i servizi di sicurezza informatica abbiano oggi un ruolo decisivo. Una delle azioni fondamentali da seguire per ridurre al minimo il rischio di attacchi informatici e non farsi cogliere impreparati è la **dotazione di antivirus di alto livello come Eset Endpoint Security.**

PERCHÈ SCEGLIERE ESET ANTIVIRUS:

- in termini di prestazioni non appesantisca il SO
- protezione multilivello pre e post esecuzione della rilevazione del virus
- supporta tutte le piattaforme Windows, Mac. Linux, Android, anche i dispositivi mobili per IOS e Android

Eccellenti Funzionalità di Eset Endpoint Security:

GESTIONE DA UNA CONSOLE UNIFICATA

Tutti gli endpoint di ESET, inclusi gli endpoint e i dispositivi mobili, possono essere gestiti da **ESET PROTECT**, una console di gestione unificata basata sul cloud.

BLOCCO DI ATTACCHI MIRATI

Le soluzioni di protezione endpoint di ESET utilizzano **informazioni di intelligence sulle minacce** in base alla relativa presenza a livello globale, allo scopo di definirne le priorità e bloccare in modo efficace le minacce più recenti, prima che si diffondano in altre parti del mondo. Inoltre, le nostre soluzioni offrono **aggiornamenti basati sul cloud** per rispondere rapidamente in caso di mancato rilevamento senza dover attendere un aggiornamento periodico.

SCANNER UEFI

ESET è il primo provider di servizi di protezione dell'endpoint ad aggiungere un livello dedicato alla **protezione dell'interfaccia UEFI** (Unifi ed Extensible Firmware Interface). ESET UEFI Scanner controlla e applica la protezione dell'ambiente di preavvio ed è progettato per monitorare l'integrità del firmware. In caso di rilevamento di una modifica, invia una notifica all'utente.

EXPLOIT BLOCKER

ESET Exploit Blocker **monitora le applicazioni generalmente sfruttabili** (browser, lettori di documenti, client di posta, Flash, Java e altre) e non si limita a ricercare specifici identificatori CVE, ma si concentra sulle tecniche di sfruttamento. In caso di attivazione, la minaccia viene bloccata immediatamente sulla macchina.

PROTEZIONE BOTNET

Botnet Protection **rileva comunicazioni dannose utilizzate dalle botnet** e, allo stesso tempo, identifica i processi incriminati. Tutte le comunicazioni dannose rilevate vengono bloccate e segnalate all'utente.

RILEVAMENTO DEL COMPORTAMENTO - HIPS

Il sistema anti-intrusione basato su host **monitora l'attività di sistema** e utilizza un set predefinito di regole per riconoscere e arrestare il comportamento sospetto del sistema.

La Cyber War è reale e lo dimostrano gli scontri in atto tra Russia e Ucraina. Fortunatamente, esistono le società di Cyber sicurezza, che ce la mettono tutta nel difenderci.

Eset ha rilevato per prima il malware Hermetic Wiper: l'attacco informatico che distrugge i dati presenti sui dispositivi.

Le minacce zero-day rappresentano una grande preoccupazione per le aziende, poiché non dispongono di una soluzione semplice per proteggersi da qualcosa che non hanno mai visto prima.

Eset dispone di 13 laboratori di ricerca e di sviluppo che consentono di rispondere e riconoscere rapidamente i malware mai visti prima. L'antivirus sfrutta l'euristica e il machine learning nell'ambito di un approccio multilivello per garantire la migliore prevenzione e protezione. **Il sistema di protezione sul cloud di ESET** garantisce protezione automatica dalle nuove minacce senza che sia necessario attendere il successivo aggiornamento dei rilevamenti.

La Network Attack Protection impedisce ai ransomware di infettare un sistema, bloccando gli exploit a livello di rete. **La protezione multilivello Eset presenta una sandbox integrata** in grado di rilevare malware che tentano di eludere il rilevamento tramite l'offuscamento. Gli utenti sono protetti dalla crittografia dei file dannosi.

Il malware fileless è una minaccia relativamente nuova e, poiché esiste solo nella memoria, **richiede un approccio diverso rispetto ai tradizionali malware basati su file**.

- **Advanced Memory Scanner**, un'esclusiva tecnologia ESET, protegge da questo tipo di minacce monitorando il comportamento dei processi dannosi ed eseguendone il controllo dopo che il mascheramento viene annullato nella memoria.
- Le minacce vengono caricate su **ESET Threat Intelligence** fornendo informazioni sulle modalità di funzionamento, riducendo il tempo di raccolta e di analisi dei dati.

Gli **attacchi hacker** possono davvero causare enormi problematiche. Non tutti gli antivirus proteggono allo stesso modo: occorre necessariamente una protezione completa.

Il mondo cambia così velocemente e gli I-TEAM sono il provider affidabile e competente per le aziende che necessitano di soluzioni tecnologiche all'avanguardia. Siamo a disposizione delle imprese per aiutarle a rimanere protette dotandole dei giusti strumenti.

LA SICUREZZA A 360°

IT SECURITY

A cura di
Paolo Vannini

Karakurt: I NUOVI CYBER CRIMINALI BEFFARDI

In questi ultimi anni i cyber criminali sono moltiplicati ad una velocità molto preoccupante, tirando su metodi di attacco sempre nuovi e sempre più dannosi. Di recente è emerso Karakurt, un gruppo criminale informatico che, negli ultimi mesi del 2021, ha colpito oltre 40 vittime accertate, ma si prospettano dati ben più alti.

La loro ironia, per un attimo, li rende quasi simpatici; ecco le loro parole:

"Se sei stato vittima di un attacco hacker e di un furto di dati, non avere fretta di incolpare il tuo team di sicurezza. Semplicemente non era la loro giornata. Il budget che spendi per l'acquisto di dispositivi di protezione ed anti-malware possono solo complicare il nostro lavoro.Non potranno mai proteggerti completamente ma noi, da parte nostra, amiamo molto i compiti complessi".

La maggior parte degli APT (Advanced Persistent Threat) sono lanciate da hacker che sono alla ricerca di un tornaconto finanziario, con ransomware rivolti ad aziende di grandi dimensioni. Karakurt si "diverte" esfiltrando dati sensibili di aziende più piccole, utilizzando credenziali VPN legittime ed accessi Anydesk (la famosa applicazione di desktop remoto) come vettore di accesso iniziale (al momento non è chiaro come riescano ad ottenere queste credenziali). La tecnica dell'esfiltrazione dei dati consiste nella copia o il trasferimento dei dati non autorizzati al di fuori del dominio dell'utente. Un esempio concreto: un account può essere violato eseguendo l'accesso passando attraverso un'app installata di terze parti che li invia all'esterno del dominio. È così che i dati possono esser sottratti. Tra i malcapitati c'è anche una società italiana che si occupa di trasporto logistico. I settori più colpiti sono quello industriale, healthcare e dei professionisti.

I·TEAM

Cinque società che si sono unite per dare forma a un grande progetto:
aiutare le imprese a crescere nella digitalizzazione
e nella rivoluzione digitale, per avere performance
sempre più efficaci ed efficienti, all'altezza dei grandi cambiamenti
dell'economia e della società contemporanea.

Allyou.srl

ego communication

GlobalNet
Servizi di Telecomunicazioni per la tua Azienda

OMEGA SISTEMI
Soluzioni Informatiche Professionali

NETWORK PRIVACY

PANTAREI INFORMATICA
La tecnologia resa semplice

WWW.I-TEAM.TECH

Via Benedetto Dei 64 · 50127 FIRENZE · Numero Verde 800-199760 · info@i-team.tech