SICUREZZA

LA PROTEZIONE DAGLI ATTACCHI INFORMATICI PASSA DAL MIGLIORAMENTO DEGLI STRUMENTI A DISPOSIZIONE DI UTENTI E ORGANIZZAZIONI, A PARTIRE DA SISTEMI OPERATIVI SEMPRE PIÙ EVOLUTI.

ECCO LE SOLUZIONI WINDOWS.

ESPRINET EXPERTS HUB

esprinet® in collaborazione con Microsoft intel.

FUTURO SICURO

L'evoluzione costante del panorama delle minacce informatiche offre sfide senza precedenti.
Aziende e organizzazioni si trovano a fronteggiare pericoli sempre più frequenti - tra tutti: phishing, ransomware e attacchi DDoS (Distributed Denial of Service) - che richiedono strategie di difesa robuste e affidabili.

UNO SGUARDO AL CONTESTO

Secondo l'Associazione Italiana per la Cybersecurity (CLUSIT), nei primi 6 mesi del 2023 il mondo ha assistito a 1382 attacchi informatici, con un'incidenza media di 230 eventi al mese.
Secondo l'Associazione Italiana per la Cybersecurity (CLUSIT), nei primi 6 mesi del 2023 il mondo ha assistito a 1382 attacchi informatici, con un'incidenza media di 230 eventi al mese. In Italia sono cresciuti del 40% in un anno, cifra che si colloca ben oltre la media mondiale dell'11%. Di seguito, alcuni dettagli rilevanti:

Principali cause e conseguenze

Gli obiettivi criminosi guidano la grande maggioranza degli attacchi.Tra le tecniche più utilizzate troviamo l'inoculazione di malware (in particolare il ransomware), e gli attacchi che mirano a sfruttare vulnerabilità esistenti.

I settori più esposti

Il settore sanitario, quello finanziario/assicurativo e l'ambito educativo sono tra i più esposti all'azione del cybercrime.
In questi ambiti si registra un aumento della gravità degli attacchi, con una percentuale che è cresciuta dal 36% al 40% in un anno per quanto riguarda quelli considerati più critici.

Il contesto italiano

Come accennato, in Italia, gli attacchi hanno segnato un incremento del 40%, con una presenza significativa di hacktivism legato al conflitto tra Russia e Ucraina.
I settori più interessati sono stati quelli della produzione industriale e del finanziario/assicurativo.

1382 attacchi
230 eventi al mese
+ 40%

Settori più esposti
Sanità
Finanza
Assicurazioni
Educazione

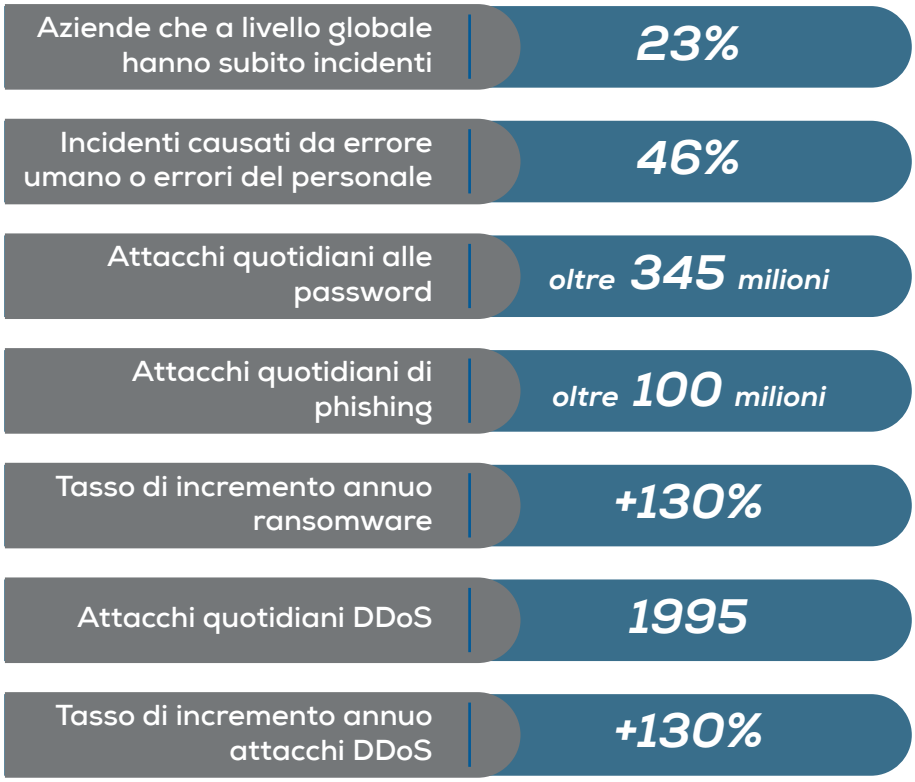
IL “TOCCO UMANO”

L'errore umano rende ancora più impegnativa questa sfida, essendo alla base del 46% di tutti gli incidenti legati alla sicurezza informatica

Fonte: Microsoft Digital Defense Report 2022

A creare occasioni di vulnerabilità è la sempre più diffusa adozione di modalità lavorative diverse e di ambienti di lavoro flessibili. La rapida digitalizzazione e il cambiamento nelle preferenze lavorative hanno infatti radicalmente trasformato la concezione tradizionale del luogo di lavoro. La flessibilità richiesta dal contesto professionale contemporaneo genera complessità e sfide in termini di sicurezza informatica, con i dipendenti alla ricerca di soluzioni semplici per collaborare e per rimanere produttivi ovunque si trovino.

SEMPRE SECONDO MICROSOFT, IL 23% DELLE ORGANIZZAZIONI HA SUBITO INCIDENTI LEGATI ALLA SICUREZZA INFORMATICA, SPESSO A CAUSA DI ERRORI UMANI O DI PERSONALE, SOTTOLINEANDO L'IMPORTANZA DI UNA DIFESA BASATA SULLA TECNOLOGIA E DI PROTOCOLLI DI SICUREZZA SOLIDI.

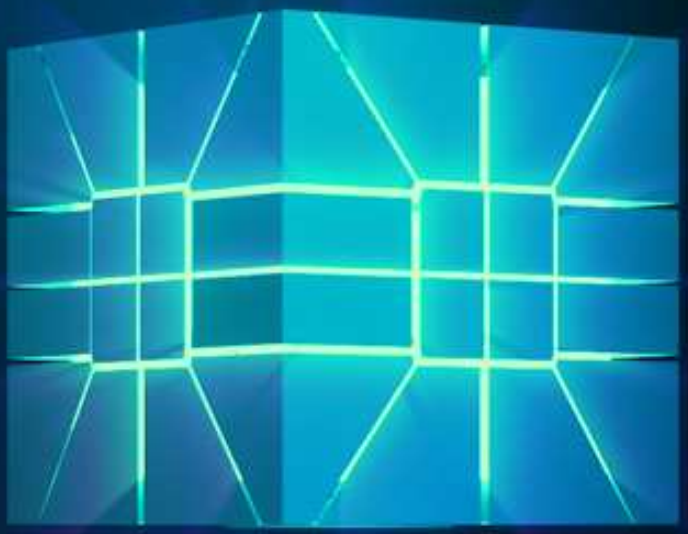


(Fonte: Microsoft)

I dati evidenziano tendenze preoccupanti.
Due emergono tra tutte: l'incremento quasi triplo, nel 2023, degli attacchi alle password, con una frequenza di 4.000 eventi al secondo; la quantità impressionante di tentativi quotidiani di phishing (101 milioni) e un aumento annuale del 130% nelle minacce ransomware.

Zero Trust

Non fidarsi mai,
verificare sempre



FUTURO DEL LAVORO E CYBERSECURITY

IL RUOLO DEL SISTEMA OPERATIVO

In una ricerca condotta con la collaborazione di LinkedIn e GitHub (New future of work), Microsoft ha evidenziato l'importanza di nuovi dispositivi e sistemi operativi nel plasmare il futuro del lavoro e nell'affrontare le sfide della cybersecurity. L'adozione di stili di lavoro flessibili - alimentata dall'accelerazione alla digital transformation impressa nel periodo della pandemia e da lavoratori sempre più orientati a ottenere maggiori autonomia e comodità - porta ad aumenti di produttività e un miglior grado di soddisfazione lavorativa.
Questi cambiamenti, tuttavia, presentano nuove sfide di sicurezza, specialmente in ambienti di lavoro flessibili.
Nell'evoluzione del lavoro gioca un ruolo sempre più importante l'intelligenza artificiale (IA), come dimostrato da tecnologie quali Windows Copilot e Microsoft 365 Copilot, che accelerano la generazione di dati.

Copilot

Dispositivi obsoleti rappresentano un ostacolo all'innovazione che queste nuove tecnologie promettono: quasi il 90% dei responsabili della sicurezza aziendale concorda sul fatto che l'hardware datato aumenti la vulnerabilità agli attacchi.
Ecco perché, per rimanere competitive, le aziende hanno bisogno di strumenti moderni e sicuri, progettati seguendo l'approccio "Secure-by-design".

NON FIDARSI MAI, VERIFICARE SEMPRE

L'evoluzione delle minacce informatiche e l'aumento del lavoro da remoto hanno reso obsoleti i perimetri di sicurezza tradizionali. Ecco perché è fondamentale implementare un framework Zero Trust, la soluzione migliore per proteggere i dati sensibili in un ambiente sempre più distribuito e per mitigare il rischio di violazioni dei dati.
A differenza dei modelli di sicurezza tradizionali, che operano secondo il principio "fidarsi, ma verificare" e considerano affidabili gli utenti e i dispositivi all'interno del perimetro di sicurezza aziendale, il modello Zero Trust adotta il principio opposto: "non fidarsi mai, verificare sempre".
Il procedimento di verifica è estremamente rigoroso: ogni tentativo di accesso a risorse di rete, indipendentemente dalla posizione dell'utente o del dispositivo, deve essere autenticato, autorizzato e crittografato prima dell'accesso. Inoltre, gli utenti e i dispositivi dispongono solo dell'accesso l'accesso necessario per svolgere le loro funzioni, limitando così la superficie di attacco e il potenziale impatto di una violazione. La rete è suddivisa in segmenti più piccoli per controllare l'accesso dettagliato e monitorare e proteggere i dati sensibili in modo più efficace. Il monitoraggio avviene senza interruzioni per identificare attività sospette o anomalie, consentendo una risposta rapida alle minacce.

SICUREZZA AVANZATA

I PC dotati del sistema operativo Windows 11 Pro sono sviluppati secondo il modello Zero Trust, e offrono livelli di protezione avanzati per le aziende moderne, rispondendo alle esigenze di sicurezza in un panorama di minacce in continua evoluzione, a partire dall'introduzione di funzionalità di sicurezza avanzate a livello di hardware.
La base è Microsoft Pluton, un processore di crittografia sicuro integrato nella CPU che garantisce l'integrità del codice e la protezione più efficace grazie agli aggiornamenti forniti da Windows Update.

Microsoft Pluton, un processore di crittografia sicuro integrato nella CPU che garantisce l'integrità del codice e la protezione più efficace grazie agli aggiornamenti forniti da Windows Update.

Altre funzionalità decisive sono legate a tecnologie di protezione dei dati sensibili (TPM 2.0), tecnologie di isolamento attive come la sicurezza basata sulla virtualizzazione (VBS), integrità del codice protetta da Hypervisor (HVCI) per una protezione avanzata del kernel.
Si tratta di soluzioni che riducono significativamente il rischio informatico, diminuendo di 3,1 volte rispetto al normale gli attacchi al firmware.

PROTEZIONE DELLE APP AZIENDALI E DELL'IDENTITÀ

Windows 11 Pro rappresenta dunque una soluzione olistica per le aziende e le organizzazioni che si avviano a entrare nel futuro del lavoro, combinando misure di sicurezza avanzate con strumenti per una gestione semplificata con l'obiettivo di migliorare la produttività e sostenere ambienti di lavoro dinamici.
La protezione delle app aziendali e delle identità sono due piani essenziali sui quali lavorare per raggiungere l'obiettivo appena menzionato.

La protezione multilivello migliora la privacy e la sicurezza dei dati.

App Control for Business

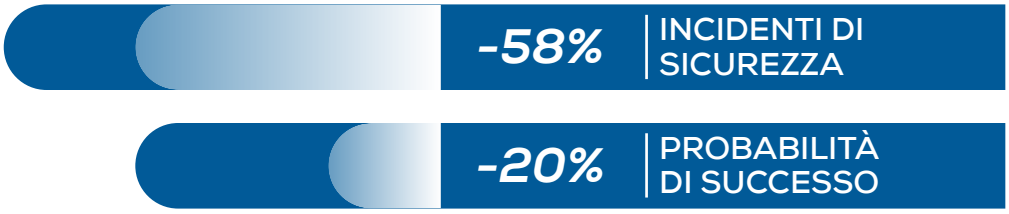
Si tratta di un sistema che offre un controllo avanzato sulle applicazioni aziendali, unito a politiche di sicurezza multilivello delle applicazioni che migliorano la privacy e la sicurezza dei dati; a ciò si aggiunge un controllo maggiore su funzionalità legate alla privacy come l'accesso a posizione, videocamera e microfono.
Insieme all'isolamento delle app Win32, ci si assicura che solo le applicazioni verificate vengano eseguite, proteggendo ulteriormente il PC dall'introduzione di malware.

Protezione delle identità

Con l'aumento degli attacchi alle credenziali, l'autenticazione multifattore e l'accesso privo di password diventano strumenti essenziali per assicurarsi adeguati livelli di sicurezza.
Windows 11 Pro li garantisce con l'adozione di Windows Hello for Business, che appunto elimina le password a favore di PIN, riconoscimento del volto o lettura dell'impronta digitale.
A ciò si aggiunge Microsoft Defender SmartScreen per una protezione antiphishing che riduce di 2,8 volte rispetto al normale il rischio di furto di identità.
Windows Presence gestisce invece la sicurezza del dispositivo grazie al blocco in caso di assenza e alla riattivazione quando ci si riavvicina.

I dispositivi che utilizzano Windows 11 Pro registrano un calo del 58% degli incidenti di sicurezza e del 20% delle probabilità di successo di quelli che si verificano.

CON WINDOWS 11



In un panorama di minacce in continua evoluzione, è cruciale che aziende e organizzazioni siano ben equipaggiate per affrontare con fiducia ed efficacia le sfide di sicurezza attuali e futuro; un futuro in cui, è bene ricordarlo, alcune delle soluzioni ora disponibili non saranno più aggiornate.
E' il caso di Windows 10, il cui supporto terminerà il 14 ottobre 2025.

Il supporto per Windows 10 terminerà il 14 ottobre 2025

In questo contesto di continua trasformazione sono quindi richieste soluzioni tecnologiche che, oltre alle esigenze di protezione, supportino anche una gestione semplificata e promuovano diversi stili lavorativi.
In questo, Windows 11 Pro emerge come una piattaforma avanzata che si estende oltre le tradizionali misure di sicurezza IT, mirando a soddisfare le esigenze complesse di protezione, produttività, collaborazione ed efficienza operativa.

PER MAGGIORI INFORMAZIONI,
CONTATTACI

DistiMicrosoft@esprinet.com

www.esprinet.it