Oggi parliamo di sicurezza.

La sicurezza è da sempre un tema caldo e oggi lo è molto di più che in passato, dato che le minacce sono aumentate in modo esponenziale e colpiscono ogni possibile area vulnerabile dei sistemi informatici: server, client, dispositivi mobili, dati, comunicazioni, applicazioni e utenti.

Per quanto riguarda i PC, Windows 11 costituisce un tassello chiave nella strategia di Microsoft per dare una risposta adeguata alle sfide attuali della sicurezza.

A questo scopo, Microsoft ha dotato Windows 11 di una serie di misure specifiche dedicate alla protezione di ognuna delle aree di vulnerabilità elencate. In questo podcast parleremo appunto di tali misure, per capire meglio se le stiamo sfruttando appieno oppure se possiamo introdurre dei miglioramenti riguardo alla protezione dei sistemi dei nostri clienti.

La prima area che abbiamo citato è quella dei dispositivi.

Lato hardware, ad esempio, sappiamo che Microsoft ha imposto alcuni requisiti di base per le macchine Windows 11: il secure boot, il firmware basato su UEFI e il TPM 2.0 sono tutti elementi fondamentali nella protezione dei PC. Chi compera una macchina nuova oggi, non dovrebbe preoccuparsi: tutti questi requisiti sono praticamente sempre soddisfatti. Sui PC un po' più datati, invece, questo non è detto e bisogna controllare che le macchine in uso li soddisfino.

Siccome sappiamo che l'hardware da solo non è sufficiente, dal lato del software, Windows 11 dispone di tutti i meccanismi di protezione di base, come, ad esempio, l'antivirus. Windows Defender, come tutti i prodotti analoghi, effettua sia la scansione periodica dei file su disco sia il monitoraggio real time dei file in esecuzione (tramite SmartScreen).

Windows 11, però, non si ferma qui: grazie alla Virtualization Based Security (VBS), ad esempio, è possibile controllare e impedire l'esecuzione di codice malevolo attraverso la cosiddetta Hypervisor-Protected Code Integrity (HVCI).

In realtà la Virtualization Based Security permette di proteggere anche altri elementi della piattaforma di sistema e in Windows 11 è molto più facile da attivare e da gestire di quanto non lo fosse in Windows 10. Per gestire la VBS e tutti i meccanismi di protezione insiti in Windows 11, infatti, si può utilizzare l'app Sicurezza di Windows, che dispone di un "cruscotto" dedicato, che offre, a colpo d'occhio, una visione globale sia delle impostazioni di sicurezza sia dello stato di salute complessivo del PC.

Riguardo alla protezione dei dati, la tecnologia fondamentale adottata è la crittografia. Anche in Windows 11, lo strumento principale da utilizzare per proteggere i dati è BitLocker, il quale, come sappiamo, permette di cifrare l'intero disco. Forse non tutti sanno, però, che BitLocker può essere usato anche per proteggere i dischi rimovibili, compresi i pen drive USB. In questo caso lo strumento si chiama BitLocker To Go e entrambi possono essere gestiti, sul singolo PC, dal Control Panel di Windows e, in ambito aziendale, si possono gestire anche centralmente, tramite Active Directory e le sue Group Policy.

Oltre alla crittografia dell'intero disco, in Windows, da tanti anni è possibile anche cifrare solo una cartella o un singolo file, su dischi formattati con NTFS, tramite l'Encrypted File System (in sigla EFS).

Sia con BitLocker, sia con EFS, la protezione di file e cartelle è legata alla posizione in cui essi si trovano. Nel momento in cui un file venisse spostato in una posizione non cifrata, la protezione non sarebbe più

Sede legale e operativa:
Via Dogana, 8/2 - 48022 Lugo (RA) - ITALY
C.F. e P. IVA IT 01250880398

Direzione, sede commerciale e amministrativa:
Tel. (+39) 0545 33355 Fax (+39) 0545 33379

Assistenza tecnica:
Tel. (+39) 0545 25911

attiva. Se si desidera, invece, legare la crittografia al singolo file, indipendente dalla posizione in cui viene salvato, ci si può avvalere di soluzioni come Microsoft Information Protection, che sono capaci di legare la protezione al singolo file e all'identità di chi richiede l'accesso e non, invece, alla posizione in cui si trova il file o alla modalità di trasferimento adottata.

Come sempre, quando si tratta di utilizzare la crittografia, è necessario porre una grande attenzione al suo impiego e predisporre sempre tutte le misure idonee a recuperare i dati cifrati in caso venga smarrita la chiave di cifratura o gli utenti non si ricordino le credenziali utilizzate all'atto della cifratura stessa.

Passando alle comunicazioni, la protezione in Windows 11, si attua tramite l'adozione di nuovi protocolli sia lato Internet sia lato client/server e tramite l'uso appropriato di Windows Firewall, il quale può essere, come BitLocker, anch'esso gestito centralmente tramite Active Directory.

Come è ormai più che evidente, proteggere solo dispositivi e dati non è sufficiente e bisogna tenere conto anche delle applicazioni e degli utenti.

Abbiamo già accennato alla presenza di Defender SmartScreen e delle soluzioni basate su VBS che sono presenti anche nell'edizione Pro; nelle edizioni Enterprise di Windows, oltre a queste, è possibile utilizzare anche strumenti più potenti, come AppLocker, che consente di creare delle regole per consentire o negare l'esecuzione di applicazioni in base all'identificativo dei file eseguibili o all'appartenenza o meno a gruppi specifici di Active Directory.

Un'altra misura di protezione fondamentale, contro l'esecuzione di codice malevolo, è Application Guard, che utilizza VBS per eseguire, all'interno di un ambiente isolato, il codice presente in siti non attendibili. In questo modo è possibile proteggere i sistemi aziendali da eventuali siti compromessi o dannosi. L'amministratore ha la possibilità di definire siti e reti attendibili per applicare la protezione a tutte le altre aree che, di fatto, risultano non essere attendibili.

Il fatto che esistano delle tecnologie che proteggono automaticamente i sistemi, tuttavia, non vuol dire che gli utenti non debbano essere istruiti riguardo ai comportamenti sicuri da tenere e agli strumenti da usare per proteggersi.

A questo scopo, ad esempio, una funzionalità poco nota di Windows 11 è la Sandbox. Non è installata di default e, una volta installata, si presenta come una app nel menu Start. Sandbox crea un ambiente Windows completamente isolato dalla macchina principale, nel quale è possibile testare, in modo sicuro, ogni tipo di applicazione senza che, in alcun modo, eventuale codice malevolo possa toccare il PC sottostante. Alla chiusura della Sandbox, infatti, tutto viene cancellato e, alla successiva esecuzione, l'ambiente riparte sempre in modo pulito. Nella futura versione della Sandbox di Windows 11 sarà anche possibile riavviare l'ambiente isolato per testare anche il software che richiede il riavvio per completare la propria installazione. Ovviamente i riavvii dovranno avvenire sempre nella stessa sessione, perché comunque, alla chiusura della Sandbox, verrà fatto un reset completo.

Windows Sandbox è una delle funzionalità di Windows, come Hyper-V, che si possono installare dal Pannello di Controllo.

Come abbiamo appena detto, parlando di "comportamenti sicuri" da parte degli utenti, non si possono certo trascurare i meccanismi di autenticazione avanzati offerti da Windows 11.

Sede legale e operativa:
Via Dogana, 8/2 - 48022 Lugo (RA) - ITALY
C.F. e P. IVA IT 01250880398

Direzione, sede commerciale e amministrativa:
Tel. (+39) 0545 33355 Fax (+39) 0545 33379

Assistenza tecnica:
Tel. (+39) 0545 25911

L'approccio cosiddetto "passwordless" riveste un'importanza particolare in questo ambito, così come, più in generale, l'autenticazione a più fattori.

La base dell'autenticazione "passwordless" per Microsoft è Windows Hello for Business, che combina un fattore biometrico (cioè l'impronta digitale, il palmo della mano, il riconoscimento facciale) e un PIN, sia col dispositivo utilizzato, sia con le credenziali dell'utente memorizzate sul dispositivo stesso.

Windows Hello for Business, associando le credenziali biometriche e il PIN al PC e integrando l'infrastruttura a chiave pubblica (PKI) e il supporto alla modalità di autenticazione in modalità Single Sign-On (SSO), offre un metodo pratico per accedere al PC, alle risorse aziendali on premises e nel Cloud, senza mai dover ricorrere alla password. In futuro, in combinazione con altre tecniche di autenticazione disponibili in Cloud, si potrà fare del tutto a meno della password stessa dato che, come sappiamo, essa costituisce l'anello più debole nella catena di protezione delle identità elettroniche.

Ultima misura da citare, non meno importante di quelle già descritte, è la cosiddetta Multi Factor Authentication, in sigla MFA. In realtà, la MFA non è immediatamente disponibile per l'accesso a un PC. Windows 11, ovviamente, come anche i suoi predecessori, supporta l'utilizzo di smart card o di token da abbinare all'uso delle credenziali; si tratta di elementi di difficile gestione e, di solito, poco simpatici agli utenti. Oggi, l'MFA si ottiene più comunemente abbinando, al dispositivo, un opportuno servizio Cloud, come ad esempio, Azure AD, e una app di autenticazione, come Microsoft Authenticator. Con le soluzioni Microsoft, se il PC fa parte dei dispositivi gestiti in Cloud dall'organizzazione di appartenenza e l'utente accede con le credenziali di Azure AD già oggi è possibile applicare delle misure di sicurezza molto stringenti anche all'atto dell'autenticazione.

Quella della protezione delle identità elettroniche è, comunque, un'area in grande evoluzione, su cui si stanno concentrando moltissimi investimenti di Microsoft. Non a caso, proprio in quest'area, è stata annunciata, poco più di un mese fa, una nuova famiglia di soluzioni dedicate alla cybersecurity denominata Microsoft Entra, all'interno della quale si collocheranno anche tutti gli elementi relativi all'identity management e alla gestione delle autorizzazioni di accesso.

Nel prossimo podcast, che costituirà il seguito di questo, vedremo anche come possiamo proteggere in modo adeguato non solo le macchine Windows 11 ma anche tutti gli altri PC degli utenti, grazie alla famiglia di soluzioni Cloud Safe di Si Computer.

Continuate a seguirci qui, sul canale SI KnowIT, per approfondire sempre di più la nostra conoscenza della piattaforma Windows e, in modo più specifico, di Windows 11

Sede legale e operativa:
Via Dogana, 8/2 - 48022 Lugo (RA) - ITALY
C.F. e P. IVA IT 01250880398

Direzione, sede commerciale e amministrativa:
Tel. (+39) 0545 33355 Fax (+39) 0545 33379

Assistenza tecnica:
Tel. (+39) 0545 25911