OsservatoriO AttacchInformatici

I PROBLEMI E LE VULNERABILITÀ LEGATE AI FENOMENI CONSUMERIZZAZIONE E BYOD

TABLET E SMARTPHIONE STANNO INVADENDO LE AZIENDE IN MODO INCONTROLLATO, APRENDO MOLTI PROBLEMI DI CUI NON SI PUÒ FAR CARICO SOLO L'IT.

M.R.A. Bozzetti, OAI founder

Negli ultimi tempi si va diffondendo il termine consumerizzazione, derivato dall'inglese 'consumerization', che indica la tendenza a usare anche per attività aziendali dispositivi e applicazioni del mondo consumer, il più delle volte di proprietà dell'utente finale.
Per indicare la proprietà non dell'azienda ma del cliente finale è stato coniato l'acronimo Byod, Bring your own device, che molti di voi avranno già sentito, ovvero: "Porta con te il tuo dispositivo". L'affermazione indica la politica di aziende/enti aperta a tollerare e/o a consentire, e in maniera crescente ora a incoraggiare/promuovere, l'utilizzo dei dispositivi privati di ICT nelle attività aziendali.
Il fenomeno non è certo nuovo, ma fino a poco tempo fa era limitato ai professionisti e alle società di consulenza e di ricerca e sviluppo, per lo più del mondo ICT e per aziende e studi di piccole e medie dimensioni. Con la diffusione dei laptop, nella maggior parte dei casi di proprietà dell'azienda/ente, questi dispositivi sono diventati il compagno inseparabile dell'utente, la sua 'coperta di Linus' sempre in uso sia in ufficio che fuori, per attività lavorative o domestiche, dai giochi ai business plan familiari e ai social network. L'ondata inarrestabile degli smartphone e dei tablet, considerati prodotti elettronici di consumo, oltre che dei laptop ultra piatti e ultra leggeri (chiamati Umpc, ultra mobile pc), e la concomitante crescente disponibilità delle reti wireless per la connessione a internet, ha velocemente portato alla consumerizzazione e al Byod, ponendo non pochi problemi per la loro gestione in ambito azienda/ente, in particolare per la gestione della sicurezza informatica.

Un impegno 'always on'

Tale esplosione non ha solo le motivazioni tecnologiche sopra evidenziate, ma anche motivazioni a livello individuale: da un lato il crescente impegno delle persone nelle attività di business, che divengono sempre più totalizzanti (quanti colleghi ed altri professionisti trovo, per esempio via Skype, in attività a tarda notte ...), dall'altro le preferenze d'uso dei dispositivi, tipiche dei prodotti consumer, che arrivano a diventare 'status symbol', soprattutto nei vertici aziendali e nella generazione millennial (o generazione Y).
Chi è abituato a usare, come utenza privata, uno smartphone, quasi si vergogna a utilizzare un normale cellulare fornito dall'azienda, a costo di alternare spesso sul proprio dispositivo la SIM aziendale e quella personale. Analogamente, se si usa a livello personale un tablet o un Umpc, ben difficilmente si usa il pc mobile 'classico' fornito dalla propria azienda/ente.
Questa tendenza è inarrestabile, e crea per le aziende/enti aspetti positivi, quali l'aumento della produttività, maggior interazione e comunicazione, fidelizzazione dei dipendenti. Ma smartphone e tablet sono pc a tutti gli effetti, ed 'ereditano' quindi tutte le vulnerabilità tipiche dei pc, alle quali si aggiungono nuove vulnerabilità e nuovi rischi comportamentali.

Le nuove vulnerabilità

Le nuove vulnerabilità dipendono in primo luogo dai sistemi operativi per smartphone, tipo Android, iOS, Symbian OS, BlackBerry

OS, Windows Phone, web OS, per i quali sono stati creati e si diffondono innumerevoli codici maligni. Per i tablet i sistemi operativi sono gli stessi dei pc. Dal punto di vista tecnico le possibili tipologie di attacco sono in pratica le stesse dei pc, con maggiori probabilità di successo dovute all'uso promiscuo personale e per lavoro.

Questo comportamento, che non ha ormai più senso bloccare e/o vietare, porta a un insieme di problemi che l'azienda/ente deve comprendere e gestire, tra i quali:

- la gestione dei dispositivi affidati o di proprietà degli utenti;
- la protezione dei dati aziendali, soprattutto quelli riservati e critici;
- l'utilizzo non controllabile di software e di dati pericolosi per l'azienda/ente.

Le realtà di medie e grandi dimensioni hanno attive, o dovrebbero avere, delle policy per la sicurezza anche sui dispositivi mobili: ma come farle rispettare se il dispositivo non è di loro proprietà, ma del dipendente? Come può l'azienda proibire al dipendente di accedere con lo smartphone o il tablet personale a certi siti e social network, o obbligarlo a installare determinati software sul dispositivo, per esempio un antivirus che dall'utente/proprietario è considerato penalizzante in termini prestazionali?

In logica consumer, l'utente può acquistare delle applicazioni, le famose app, scaricabili e pagabili online da magazzini software pubblici, quali per esempio App Store, Google Play, Windows Phone Marketplace, BlackBerry App World.

Ma quali di queste app soddisfano le policy aziendali? Come distinguere i costi di acquisto delle app in carico all'azienda rispetto a quelli personali? Come verificare che le app siano intrinsecamente sicure e non abbiano al loro interno codici maligni?

I rischi sono alti e seri per l'azienda. Si pensi per esempio alla possibile esposizione a terzi non autorizzati di dati aziendali critici, causata dalla perdita o dal furto del dispositivo, oppure perché acceduti o trasmessi, senza intenzione dolosa da parte dell'utente, tramite social network, web mail o altri canali di comunicazione non aziendali.

Cosa fa e cosa non fa l'IT

L'enorme numero di app disponibili, oltre all'elevato numero di operatori wireless utilizzato dalle aziende che operano soprattutto in più Paesi, rendono praticamente proibitivo un efficiente ed efficace supporto da parte dell'IT aziendale e dall'help desk.

Per il responsabile dei sistemi informativi e per il responsabile della sicurezza informatica la consumerizzazione può rappresentare un reale incubo: la soluzione più facile sarebbe proibirla, ma questo non è fattibile e potrebbe essere controproducente; come proibire la consumerizzazione ai vertici aziendali che di fatto l'hanno attivata? Come dire all'amministratore delegato e ai direttori centrali di usare smartphone e tablet separati per l'uso aziendale e per quello privato? La consumerizzazione ben difficilmente è bloccabile in una moderna struttura organizzativa; va invece gestita con buon senso.

Come agire

Alcuni suggerimenti, derivati dalle prime esperienze concrete adottati dalle aziende che hanno già affrontato il problema, possono essere utili per il responsabile dei sistemi informativi.

Un primo passo è prendere coscienza del fenomeno e informare i vertici dell'organizzazione, possibilmente con una proposta operativa: non si deve solo evidenziare un problema, bisogna anche proporre una sua soluzione valutando tempi, costi e ritorni. In tal senso occorre ripensare e modificare le policy sui dispositivi mobili e sulla loro sicurezza, possibilmente dopo aver svolto un'indagine-censimento dei dispositivi mobili usati dai dipendenti. Il coinvolgimento dell'utenza è determinante.

Su tale base conoscitiva sono poi definibili gli standard interni dell'architettura ICT che distingueranno tra i dispositivi mobili considerati 'enterprise standard', totalmente supportati dall'IT, da quelli ammessi, supportati congiuntamente con l'utente finale, e che potranno accedere solo ad alcune applicazioni corporate, e non ad altre: per esempio alla posta elettronica ma non all'ERP.

Per i dispositivi enterprise standard e per le reti wireless dovranno inoltre essere stabiliti contratti e accordi con i diversi fornitori per cercare di omogeneizzare i livelli di servizio necessari per l'azienda/ente.

Dovranno infine essere attivati gli opportuni strumenti informatici di controllo e di supporto ai diversi dispositivi mobili.

Marco Bozzetti,