SOPHOS

simple + secure

Sicurezza dei dispositivi **mobili**: che cosa ci riserva il **futuro**?

La rivoluzione dei dispositivi mobili è con tutta probabilità il cambiamento più significativo nell'ambito dell'informatica, dal superamento del mainframe, avvenuto oltre vent'anni fa. Questi dispositivi palmari abilitano la connessione da qualsiasi posizione geografica, l'accesso costante alla più grande banca dati di tutto lo scibile umano, nonché un potere informatico superiore a quello della sala di controllo della NASA durante il primo atterraggio sulla luna.

Ma che cosa ci riserva il futuro, e quali sono le implicazioni in termini di sicurezza?

Il vostro telefonino sa dove siete, dove dovreste trovarvi e con chi dovreste parlare. Siamo ora in grado di collegare nel giro di pochi istanti le nostre vite reali alle informazioni digitali, con: l'acquisto di biglietti, la condivisione di dati d'affari, o il contatto con amici che si trovano nelle vicinanze.

I dispositivi mobili, con il loro rapido sviluppo e la loro celere innovazione, già permettono a professionisti e utenti che lavorano da casa di gestire gli affari e le proprie vite private in movimento. In aggiunta, aprono nuove finestre su una serie di servizi e modelli d'affari innovativi. Con le loro caratteristiche, rappresentano il cardine della futura crescita economica. Tanto di cappello agli sviluppatori di hardware e software mobili: le tecnologie moderne sono straordinarie.
Ma quali sono le principali forze portanti dell'evoluzione della tecnologia mobile? Che cosa ci riserva il futuro, e quali sono le implicazioni in termini di sicurezza?

Nuove tecnologie, nuovi problemi di privacy e sicurezza

È inevitabile che i dispositivi mobili diventino sempre più potenti e più integrati nelle nostre vite private e lavorative. Il maggiore potere informatico e le dimensioni più ridotte fanno di questi dispositivi un'alternativa sempre più fattibile ai PC tradizionali, piuttosto che un semplice strumento accessorio. Molti di noi già li usano in questo modo per una notevole parte della giornata. Possiamo anche prevedere un'ulteriore diversificazione dei fattori di forma; il tablet PC ha già riscontrato un enorme successo, ma seguiranno altre soluzioni. Questi nuovi fattori di forma dei dispositivi mobili contribuiranno a rendere ancor più sfumati i confini fra PC e dispositivi mobili.

Mentre la maggior parte di noi cerca di difendersi dagli attacchi tradizionali su questi dispositivi, come malware e phishing (e non vi è alcun dubbio che tali rischi esistano), le nuove funzionalità generano ulteriori opportunità per i malintenzionati.
Le nuovi funzioni, come ad es. realtà aumentata, riconoscimento facciale ed integrazione dei social media, potrebbero esporre gli utenti a nuovi tipi di violazione. La realtà aumentata connette, per esempio, le informazioni relative all'ubicazione dell'utente con i suoi "amici" sui social media, permettendo così di identificare i contatti digitali nelle vicinanze. Non so voi, ma personalmente io sono molto più cauto a stringere amicizie nella vita reale di quanto non lo sia con le connessioni digitali.
A sua volta, ciò spalanca nuove prospettive di ingegneria sociale, come ad es. dedurre quando non vi trovate a casa, allo scopo di commettere crimini (è questo che fanno siti come PleaseRobMe.com). Una tecnica dell stesso stampo, il riconoscimento facciale e la pratica di taggare utenti nelle foto dei siti di social media, confonde ancor di più il confine fra vite personali e lavorative. Ad esempio, alcuni agenti di polizia sono già stati vittime di attacchi, in seguito alla violazione delle loro identità tramite l'uso di social media e tecniche di riconoscimento facciale.

NFC (Near Field Contact) è un altro interessante esempio di tecnologia innovativa che si prefigge lo scopo di facilitare le azioni dei consumatori. Introduce però una nuova dimensione di sfide per i professionisti della sicurezza; i dispositivi mobili diventano un obiettivo molto più interessante per il furto di denaro. È presente una sempre più forte tendenza ad incorporare la tecnologia NFC nei dispositivi mobili, la quale permette agli utenti di effettuare pagamenti o di trasferire informazioni personali facendo scorrere un dispositivo mobile su un lettore. Il telefonino assumerà sempre più le sembianze di un unico dispositivo all'origine della maggior parte dei vari aspetti della vostra vita; ciò lo rende un obiettivo ancor più allettante per i criminali informatici.

Più dati sono resi disponibili tramite i telefonini, più strumenti diamo ai malintenzionati per progettare attacchi creativi, ideati allo scopo di compromettere le nostre vite private, i nostri affari e le nostre finanze. Parallelamente, più applicazioni e funzioni utilizziamo, più aumentiamo la superficie d'attacco. La sicurezza non è l'unica vittima: ne risentirà anche la privacy. Con l'utilizzo sempre più diffuso di queste tecnologie per questioni di praticità, è facile prevedere che le nostre vite saranno soggette ad un maggiore livello di sorveglianza; a loro volta, i cellulari diverranno una combinazione fra passaporto, archivio di dati personali e vita sociale.

Un'attitudine diversa

Insieme a questi radicali cambiamenti nelle tecnologie, sono cambiate anche le aspettative in termini lavorativi. Solamente pochi anni fa, le aziende volevano bloccare i social media ed i dispositivi non standard e non gestiti. Oggi come oggi, cerchiamo tutti consciamente di adeguarci a queste tecnologie; basta osservare il numero di aziende aventi team di dipendenti che si dedicano esclusivamente alle attività di social media come canale di marketing. Un netto contrasto con gli anni precedenti.

Questi cambiamenti nelle aspettative tecnologiche e lavorative implicano la necessità di adottare una nuova attitudine verso la sicurezza informatica. Chi non si adegua rimane tagliato fuori. Questa nuova attitudine influisce anche sul futuro della mobile security e sulle sue applicazioni: la risposta più comune alle nuove tecnologie sta diventando sì, piuttosto che no.

Applicazioni mobili, browser e fat client

Anche i dispositivi mobili hanno scombussolato le tecnologie utilizzate per creare applicazioni. Negli ultimi anni, le applicazioni basate sui browser hanno cominciato a rappresentare una sfida per i fat client tradizionali. Ciò è dovuto principalmente alla loro capacità operativa multi-piattaforma, ed al fatto che vi si può accedere da qualsiasi luogo (o dispositivo). Le applicazioni mobili locali sono ora molto numerose, con una crescita incoraggiata dalle strutture per il rapido sviluppo delle applicazioni: creare un'applicazione è facile, ed è per questo motivo che per tutto esiste un'applicazione. Queste applicazioni possono anche contenere vulnerabilità, ed è stato provato che spesso non vengono applicate neanche le più fondamentali migliori pratiche tradizionali; ad esempio, sovente le password e i dati degli utenti non sono cifrati correttamente (o addirittura per nulla). Molto spesso, per queste funzioni i fat client ed i browser client offrono API (Application Programming Interfaces) e servizi sicuri che, dopo anni di problematiche, vengono ora utilizzati da molti (anche se non ovunque). Tale tendenza si riscontra sempre più sovente anche nei sistemi operativi mobili; tuttavia gli sviluppatori non sembrano ancora utilizzarli in maniera regolare. A causa della mancanza di trasparenza, non è chiaro quanto siano completi i controlli di qualità delle applicazioni come quelli di Apple.
I cosiddetti "giardini murati" sostengono di essere in grado di tenere

alla larga le applicazioni malevole; tuttavia in diversi casi la protezione delle applicazioni sembra avere lacune di difesa. Negli anni a venire, si prevedono più sfide da risolvere a livello delle applicazioni.

Un'architettura diversa per tempi diversi

I dispositivi mobili non sono semplicemente una versione di dimensioni ridotte del PC tradizionale, sebbene svolgano operazioni sempre più simili. I loro sistemi operativi, da Android ad iOS, sono progettati in maniera radicalmente differente da quelli dei PC e le aziende produttrici hanno introdotto nuovi concetti che si basano su quanto imparato dai sistemi operativi tradizionali, nel corso di diversi anni di sviluppo dell'informatica.

Le attuali piattaforme mobili tendono ad includere funzionalità come le tecnologie di "sandboxing", che sono in grado di isolare le applicazioni. Anche i sistemi di controllo e permessi hanno subito un mutamento radicale, rispetto ai sistemi operativi tradizionali. Invece di un sistema di permessi basato sull'accesso ad oggetti scelti arbitrariamente (come ad es. le chiavi di registro), ci si concentra più sui permessi d'accesso secondo criteri umani: ovvero, per esempio, se un'applicazione richieda o meno di accedere ai dati relativi alla posizione geografica dell'utente, o agli SMS. Tali funzionalità mostrano segni molto promettenti per la creazione di un sistema operativo più sicuro e funzionale; tuttavia sono, al momento, ben lungi dall'essere perfette. Molti di questi controlli non includono impostazioni predefinite intelligenti e sicure, oppure contano sull'iniziativa dell'utente per modificare i permessi di installazione di un'applicazione (un problema che pone domande a cui non si sa rispondere; in aggiunta, noi tutti conosciamo bene la tendenza degli utenti a cliccare su 'OK' senza riflettere). Tuttavia queste funzionalità non sono solamente foriere di cattive notizie, in quanto i vendor di software di sicurezza possono gestirle ed utilizzarle per consolidare le misure di protezione dei dispositivi.

Anche i dispositivi mobili cominciano a definire la propria architettura, sulla base delle moderne prassi lavorative; BlackBerry ha, ad esempio, introdotto una funzione che prevede la coesistenza di due ambienti operativi isolati all'interno dello stesso dispositivo, permettendovi di mantenere separati i dati lavorativi e quelli personali.
Ciò offre il beneficio di un ambiente lavorativo fidato e sicuro, insieme alla flessibilità di poter utilizzare giochi ed applicazioni simili. Queste funzionalità non sono ancora diffuse, e la solidità della sicurezza fornita non è ancora stata comprovata; tuttavia, mostrano pur sempre una tendenza positiva, che potrebbe portare a migliori soluzioni di protezione per gli utenti remoti moderni.
Queste funzionalità, combinate con le offerte di prodotti dei vendor di software di sicurezza, potrebbe aprire nuove prospettive in termini di dispositivi di facile utilizzo e generalmente più sicuri.

Malware, hacking e phishing

Si sono riscontrati casi di codici malevoli per una varietà di piattaforme, ma sono comunque un numero irrisorio, se paragonati a quelli ideati per attaccare i PC tradizionali. È in particolar modo Android ad aver subito la maggior parte degli attacchi di malware, per via del suo mercato delle applicazioni più aperto; tuttavia, anche sistemi dalla forte reputazione in termini di sicurezza (come ad es. BlackBerry) ne sono caduti vittima.
Se da un lato gli attacchi del malware rivolti ai dispositivi mobili sono senza dubbio diversi, sono pur sempre possibili.
Finora, il malware dei dispositivi mobili è stato notato nella forma di applicazioni fasulle di Internet banking, le quali si appropriano delle vostre credenziali e dei vostri fondi, ed in alcuni casi anche del codice token di autenticazione inviato tramite SMS dalla banca.
Molti danno per scontato che questi dispositivi posseggano un livello di sicurezza estremamente elevato, in quanto non hanno mai subito attacchi di malware. In realtà, è solo di recente

che la maggior parte degli utenti ha cominciato ad archiviarvi dati degni di essere rubati. Ora che su questi dispositivi vengono archiviate risorse di importanza finanziaria (siccome vengono sempre più spesso utilizzati come sostituto part-time del PC), abbiamo attirato l'attenzione dei malintenzionati. Negli anni a venire, è prevedibile un incremento del volume del malware che prenderà di mira questi dispositivi. Le funzionalità antivirus saranno estremamente importanti, sebbene le tecnologie di protezione operino in maniera diversa da quelle del PC, concentrandosi principalmente su reputazione e comportamenti, piuttosto che sulla classica sicurezza dei contenuti.

Enti di vigilanza, conformità e dispositivi mobili

Ultimamente gli standard degli enti di vigilanza e di conformità hanno subito una serie di riforme a velocità vertiginosa, aumentando il potere d'azione degli enti di vigilanza ed innalzando i requisiti di conformità, per renderli più espliciti in termini di condizioni da soddisfare per controlli come la cifratura completa del disco. Questi standard sembrano essere principalmente rivolti ai PC come vettore principale della perdita dei dati, nonché alla sua posizione di fulcro tradizionale per l'investimento di fondi per la sicurezza informatica. Se però si esaminano gli standard e le leggi in questione, si nota che sono stati scritti in maniera generica, e che possono essere applicati altrettanto legittimamente ai dispositivi mobili: il fattore di forma della tecnologia utilizzata non rappresenta un'attenuante in caso di perdita dei dati.

È anzi vero il contrario: man mano che si verificano casi di perdita dei dati tramite dispositivi mobili, gli enti di vigilanza vi presteranno maggiore attenzione; in futuro si noteranno con tutta probabilità maggiori sanzioni e regolamenti specifici. Oggi come oggi, siamo comunque consci del fatto che, rispetto ai PC, i dispositivi privi dei più fondamentali controlli di conformità possono rappresentare un rischio altrettanto (se non addirittura più) serio per la conformità alle normative di protezione dei dati. I requisiti di controllo ed i criteri potranno anche essere identici, ma sui dispositivi mobili vi saranno differenze significative in termini di implementazione.

Il passo di sviluppo ed innovazione

La sfida più ardua affrontata dalla sicurezza dei dispositivi mobili è con tutta probabilità il passo di sviluppo ed innovazione delle piattaforme mobili. Ove i computer tradizionali si evolvono nel corso di un ciclo di, al massimo, 18-24 mesi, le piattaforme mobili subiscono modifiche significative ogni 3 mesi.

Da questa rapidità, sorge il problema che le nuove applicazioni ed i nuovi modi di condividere i dati verranno spesso adottati da un notevole numero di persone, ben prima che gli esperti di protezione informatica abbiano la possibilità di testarli e comprenderne le implicazioni in termini di privacy e sicurezza. In qualità di professionisti della sicurezza, abbiamo il dovere di continuare a rivalutare i dispositivi e le applicazioni in questione, per identificare l'evoluzione di nuovi rischi. Le soluzioni di sicurezza devono essere ideate per essere agili, e vanno aggiornate il più rapidamente che mai, man mano che vengono alla luce nuovi problemi. La sicurezza informatica è un servizio in costante evoluzione.

Detto questo, mentre le applicazioni ed i servizi dei dispositivi vengono sovente aggiornati automaticamente, i loro aggiornamenti del sistema operativo richiedono spesso una scomoda connessione via cavo, oppure l'interazione da parte dell'utente. Ciò rappresenta un rischio concreto di lasciare questi dispositivi in balia delle vulnerabilità, a causa della mancanza di aggiornamenti.
Il jailbreaking degli iPhones è un ottimo esempio di “malware voluto

dall'utente" che sfrutta tali lacune. Il jailbreaking consente agli utenti di personalizzare il loro dispositivo più di quanto non lo permetta Apple, nonché di eseguirvi copie pirata delle applicazioni; è una pratica piuttosto diffusa. Queste stesse lacune di sicurezza possono essere usate anche per malware indesiderato! L'infrastruttura per l'aggiornamento e l'applicazione di patch di sicurezza sui cellulari ha molto da imparare dall'industria del computer tradizionale. Forse si dovrebbero esaminare le lezioni che Microsoft ha dovuto imparare in questo ambito nel corso degli anni.

Il problema della percezione dell'utente

È ormai da tempo che utilizziamo gli smartphone; di conseguenza, ci siamo rapidamente abituati all'acquisto di applicazioni e musica, o persino all'uso di Internet banking. È interessante notare che i dispositivi mobili sembrano non porre gli stessi problemi di sicurezza dei PC, agli occhi degli utenti finali, che sembrano sentirsene immuni.
Personalmente, sospetto che ciò sia frutto dell'aver notato truffe o malware sui PC, ma non sui dispositivi mobili.

Il problema è che gli utenti possono considerare questi dispositivi completamente sicuri, mentre in realtà è solamente una questione di tempo, prima che ricevano maggiore attenzione da parte dei criminali informatici.

Quando si verificherà un'inversione di tendenza, ed i dispositivi mobili verranno presi maggiormente di mira, potrebbe esserci un notevole tempo di ritardo nella formazione della maggior parte degli utenti in materia di minacce informatiche. Molte delle aziende da me visitate sono in possesso di criteri di utilizzo accettabile e programmi di formazione sulla sicurezza, i quali indicano agli utenti come proteggere i dati ed evitare compromessi. Tuttavia, capita spesso che tali programmi di formazione non includano anche i dispositivi mobili. Per evitare di rimanere indietro, è necessario accertarsi di aver modernizzato i propri corsi di formazione per la sensibilizzazione degli utenti, e che i dipendenti si occupino subito della sicurezza dei dispositivi mobili.

IPv6 e le reti

I dispositivi mobili hanno subito una serie di upgrade della connettività estremamente significativi: da GSM a 1G, 2G, 3G, 3.5G ed ora 4G. Ed in questo momento, in tutto il mondo sono in corso importanti upgrade delle reti mobili, che permettono ai dispositivi mobili una connettività dalla velocità pari (se non superiore) a quella della banda larga. Un miglioramento estremamente utile agli utenti mobili (che in molte aziende rappresentano sempre più una tipologia standard di utente). Tuttavia, questi cambiamenti introducono anche un'interessante sfida per la sicurezza: una connettività possibile da qualsiasi luogo geografico rende i dispositivi mobili un bersaglio molto allettante per le botnet e le tecniche di comando e controllo; prima di ciò, sarebbero state tutt'altro che ideali.

I dispositivi mobili e gli operatori di telecomunicazioni sono di fatto uno dei principali clienti di IPv6: il protocollo di ultima generazione, ideato per connettere su vasta scala le reti e Internet. (Per ulteriori informazioni su IPv6, consultare questo white paper: www.sophos.com/en-us/security-news-trends/security-trends/why-switch-to-ipv6). Il numero sempre più elevato di dispositivi mobili rende la scalabilità difficile per gli operatori di telecomunicazioni.
IPv6 fornisce non solo caratteristiche per l'aumento del livello di prestazioni, ma offre anche nuove funzionalità, appositamente studiate per dispositivi mobili e protezione.

Funzioni come l'indirizzo IP mobile in IPv6 sono ideate per facilitare il passaggio dei dispositivi da una rete ad un'altra (per esempio Wi-Fi e 3G), pur fornendo lo stesso indirizzo IP "mobile". Ciò si traduce in connettività costante e migliore ricezione; in più, consente un routing efficiente per i "guerrieri della strada" ad elevata mobilità. Sono stati apportati anche diversi miglioramenti della sicurezza. Va notato che anche IPSec, lo standard di settore per le connessioni VPN sicure, è stato creato su IPv6, per poi essere trasferito ad IPv4; su IPv6, la sua implementazione è obbligatoria e nativa.

I dispositivi mobili possono essere una forza portante del cambiamento all'interno del networking; ma questi cambiamenti recano con sé anche nuove sfide di sicurezza,

e nuove tecniche da imparare per i professionisti della sicurezza informatica. Molti dispositivi mobili e tablet presenti sulla vostra rete si servono di IPv6 come impostazione standard; ciò li rende potenzialmente vulnerabili agli attacchi, se il problema non viene affrontato.

(Si prega di) Mettere in pratica le lezioni imparate

In questo settore, abbiamo imparato una serie di lezioni su come creare software a prova di attacco, progettare soluzioni dalle impostazioni sicure e dare la possibilità ai vendor di protezione informatica di produrre soluzioni di sicurezza. Per molti anni, i vendor e le aziende hanno goduto di una relazione relativamente favorevole con i tradizionali vendor di sistemi operativi; ciò ha permesso la produzione dei controlli di sicurezza richiesti. Sebbene il tutto sia ben lungi dall'essere perfetto, sono stati compiuti dei progressi.

Stiamo ora effettuando la transizione verso un nuovo ecosistema di vendor, che include Google ed Apple (per nominarne solo un paio). È essenziale che questo nuovo ecosistema metta in pratica le lezioni imparate dalla nostra esperienza con i desktop, invece di far regredire i dispositivi agli anni '90. In molte occasioni, lo sviluppo della mobile security è stato ostacolato dalla mancanza di API (Application Programming Interfaces), o dal fatto che la protezione rappresentasse un requisito fondamentale di questi nuovi vendor. Tutti noi abbiamo il compito di spronare chi di dovere, al fine di ottenere impostazioni predefinite sicure da questo nuovo ecosistema di vendor, e consolidare il concetto che le funzionalità di protezione fanno parte dei requisiti di base di un dispositivo.

Gli strumenti di sicurezza del futuro

In futuro, le soluzioni di mobile security richiederanno un mix di funzionalità proprie di dispositivi, sistemi operativi e vendor, tutto in un'unica soluzione integrata. Alcune di queste funzionalità verranno fornite dall'hardware (ad es. la cifratura completa dei volumi) o dal sistema operativo (per es. il sandboxing) del dispositivo, ma verranno gestite dai vendor di sicurezza, i quali ne riceveranno i report. Si richiederanno anche maggiori funzionalità antimalware, sebbene, come già sottolineato, non saranno le stesse dei PC. L'ambito più interessante è con tutta probabilità quello della prevenzione della perdita dei dati, DLP; grazie ad essa è possibile evitare quegli imbarazzanti errori di inoltro delle e-mail alle persone sbagliate, nonché la cifratura continua di tutti i dati, man mano che vengono trasferiti fra i vari dispositivi, siano essi telefonini, PC, o altro.
La gamma di soluzioni di protezione dei dispositivi mobili crescerà con l'andare del tempo, fino a diventare pari a quella dei PC; il perimetro di applicazione si baserà però sui dati, anziché sulla rete.

Come pianificare una strategia per la sicurezza dei dispositivi mobili

Sebbene per anni alcuni non abbiano previsto altro che catastrofi in questo ambito, la mobile security non ha riscontrato molti fenomeni degni di nota. I recenti eventi e cambiamenti nel campo delle tecnologie mobili sembrano però suggerire che con tutta probabilità le minacce a cui sono esposti questi dispositivi diverranno a breve termine più svariate e numerose; dobbiamo quindi essere pronti ad affrontarle.

Nel complesso, l'attuale mercato della mobile security è relativamente acerbo, e c'è ancora molto lavoro da fare per sviluppare i giusti controlli di sicurezza da applicare. Cominciare con il concetto di una sicurezza a 360 gradi per i cellulari che sia equivalente a quella dei desktop (inclusi AV, DLP, HIPS, cifratura, controllo delle applicazioni e così via) può essere allettante; ma in realtà queste funzioni non sono ancora disponibili su grande scala, né, in molti casi, fattibili.

La priorità va data al tenere sotto controllo i principi basilari; nonostante il clamore provocato, la maggior parte dei casi di violazione dei dati avviene a causa di pecche nella configurazione di base: password deboli, mancanza di cifratura e patch, oppure vulnerabilità alle tecniche di ingegneria sociale. Per ulteriori informazioni su come proteggersi, visitare sophos.com. Con il passare del tempo, si verificherà un'evoluzione delle minacce ai dispositivi mobili e dei controlli di sicurezza disponibili; Sophos sarà pronta a fornire ai clienti funzionalità pertinenti ed aggiornate, a seconda delle loro esigenze.

Alcuni consigli sull'approccio da adottare per la vostra strategia di

mobile security a lungo termine:

1. L'aspetto più cruciale della vostra strategia a lungo termine è con tutta probabilità l'approccio da adottare quando la strategia stessa va aggiornata o modificata. I dispositivi e le tecnologie mobili subiranno cambiamenti con una velocità incredibile, e l'evoluzione di questa ampia gamma di tecnologie è troppo imprevedibile. Lo sviluppo di una strategia informatica tradizionale di 3-5 anni non è quindi consigliabile. I team di progetto che si occupano dell'approvazione dei dispositivi mobili devono ideare una strategia di 6 mesi, utilizzando una metodologia agile e rivalutando continuamente i cambiamenti dei dispositivi stessi ed i nuovi rischi che possono introdurre.
2. Pianificate i requisiti di conformità alle normative, affinché prevedano un'inclusione più esplicita dei dispositivi mobili.
3. Accertatevi quindi che qualsiasi soluzione e tecnologia adottata (come ad esempio la gestione dei dispositivi) fornisca quanta più generalizzazione possibile in termini di tipo di dispositivo e sistema operativo. I dispositivi più in uso cambiano rapidamente, e voi avrete bisogno di impermeabilizzare ulteriormente i vostri controlli di sicurezza, per renderli il più efficaci possibile. Con l'approvazione di cinque volte il numero dei dispositivi, si corre il rischio di incrementare proporzionalmente i costi e la difficoltà di gestione. Esortate i vostri vendor a risolvere questo problema, richiedendo il supporto di piattaforme multiple.
4. Esaminate attentamente la presenza simultanea di dati lavorativi e personali sui dispositivi mobili. Questi dispositivi rappresentano spesso uno scenario estremo, in quanto mescolano contatti, indirizzi e-mail e dati in un'unica interfaccia utente, con un bassissimo livello di differenziazione per l'utente finale. Tenete costantemente presente questo fatto per la vostra strategia, in quanto è una tendenza che probabilmente continuerà. Implementate processi, criteri e regole di buona prassi, per aiutare gli utenti ad evitare di commettere errori futili, che possono compromettere gli utenti stessi e la vostra azienda.
5. Investite nella creazione di un mindshare con i vostri utenti, per catturare il massimo dell'attenzione in termini di mobile security. È necessario che capiscano il valore delle informazioni (personali e lavorative) archiviate sui loro dispositivi, e devono comprendere che questi cellulari non sono completamente sicuri. Ciò consoliderà le vostre difese, di fronte all'evoluzione dei vettori di attacco.
6. Mirate a concetti ampi. Non siate troppo specifici nel definire i dispositivi mobili: ogni giorno vede l'evoluzione di fattori di forma diversi, e la vostra strategia deve essere in grado di includere tablet, smartphone, e potenzialmente altri dispositivi incorporati. Detto questo, potrebbe essere una buona idea compilare un elenco specifico di dispositivi autorizzati; molte aziende, per esempio, consentono versioni specifiche di un sistema operativo, che includono i requisiti minimi in termini di funzionalità di sicurezza. Più si evolvono i dispositivi, più si allungherà l'elenco.
7. Chi non si adegua rimane tagliato fuori. Il rifiuto completo di questi dispositivi e queste tecnologie da parte della maggior parte delle organizzazioni non è sostenibile. Molte si trovano costrette ad accettarlo. Permettere l'uso nella vostra azienda di alcuni dispositivi, come l'iPad, dotati di un adeguato livello di sicurezza limiterà il rischio che gli utenti si servano di tecnologie più pericolose.
8. Restate sintonizzati. Sophos rilascerà nuovi controlli di mobile security, mantenendo il passo con l'evoluzione delle piattaforme e dei problemi da esse presentati. I clienti che scelgono le nostre funzionalità di mobile security non ricevono semplicemente una soluzione di mobile security definitiva, bensì intraprendono un viaggio nella risposta all'evoluzione dei problemi.

James Lyne,
Director of Technology Strategy,
Sophos @jameslyne

Boston, USA | Oxford, Regno Unito

SOPHOS