Sicurezza dei dispositivi mobili e BYOD

Author : Cesare Gallotti

Date : 6 giugno 2018

Questo articolo prosegue la serie dedicata a temi su cui ci sono i maggiori dubbi e perplessità sulle norme della serie ISO/IEC 27000.

La ISO/IEC 27001 ha un controllo specifico per i dispositivi mobili, ma solo relativo alle regole sul loro uso. Non fa esplicito riferimento alle tecnologie disponibili per controllare le impostazioni di sicurezza di questi strumenti, né al fenomeno del BYOD.

Questo ci permette di parlare, come conclusione, anche dei rischi che si vogliono nascondere.

Regole per i dispositivi mobili

Le organizzazioni devono specificare le regole (*policies,* in inglese) per l'uso dei dispositivi mobili (tra cui cellulari, tablet e pc portatili).

Alcune regole sono tipiche di ogni dispositivo informatico:

- controllo degli accessi con user-id e password (o altri meccanismi di identificazione e autenticazione);
- blocco quando non utilizzato;
- installazione e aggiornamento di antivirus;
- divieto di installare software (app per dispositivi mobili) non autorizzato.

Altre regole riguardano i dispositivi portatili nello specifico:

- evitare di visualizzare dati riservati in luoghi pubblici e quando sono facilmente leggibili da persone non autorizzate (in caso di cellulari, evitare di discutere di argomenti riservati in luoghi pubblici);
- evitare di farli usare ad altri;
- impostare la cancellazione remota dei dati in caso di furto o perdita;
- cifrare i dati.

Per i dispositivi messi a disposizione dell'organizzazione (i cosiddetti "cellulari aziendali"), anche se non richiamati dalla ISO/IEC 27001, sono oggi a disposizione degli strumenti di *mobile device management* o *MDM*, che permettono di stabilire centralmente le configurazioni dei dispositivi, esattamente come per i pc in rete. È importante ricordare quanto questi strumenti siano oggi fondamentali, visto che spesso tutte le informazioni dell'organizzazione (incluse le email con i loro allegati) sono archiviate in questi dispositivi e non solo sui pc (fissi o portatili).

Visto che la ISO/IEC 27001 non menziona esplicitamente questi strumenti, alcuni prevedono di aggiungere un controllo alla propria Dichiarazione di applicabilità; altri preferiscono vederli come casi particolare del già esistente controllo "A.06.02.01 Politica per i dispositivi portatili".

Bring your own device (BYOD)

Il termine BYOD indica un fenomeno degli ultimi 10 anni, esploso soprattutto con la diffusione degli *smartphone* e dei *tablet*: le persone usano sempre più i propri dispositivi personali per accedere ai dati di lavoro. Configurano il proprio dispositivo per ricevere e visualizzare le email aziendali e i loro allegati e per interagire con i colleghi, i clienti o i fornitori con strumenti di *instant messaging*.

In questi casi i dati devono avere lo stesso livello di sicurezza di quando sono trattati con strumenti messi a disposizione dall'organizzazione. Pertanto gli utenti devono configurare i propri dispositivi personali nello stesso modo e devono ricevere opportune istruzioni (in breve, un regolamento interno può elencare le misure di sicurezza da configurare sui propri dispositivi se usati per trattare dati dell'organizzazione).

Per inciso, consentire il BYOD con strumenti non adeguatamente protetti può avere come conseguenze la perdita o diffusione non autorizzata di dati personali, sanzionabile come previsto dal GDPR.

Inutile nasconderlo: poche persone, nella realtà, configureranno i propri dispositivi personali con misure di sicurezza sufficientemente robuste. In alcuni casi, addirittura, aprono ulteriori vulnerabilità, per esempio sincronizzando l'email aziendale con quella personale su servizi cloud pubblici (e spesso offerti da società negli USA).

Una soluzione drastica è quella di vietare il BYOD. Questo implica anche il blocco di strumenti quali webmail e di file sharing, oltre ai sempre più diffusi strumenti di *office automation* sul *cloud* (i più celebri sono quelli di Google). Infatti, fornire agli utenti strumenti cui si può accedere da qualsiasi dispositivo equivale a consentire il BYOD.

Un'altra soluzione è l'adozione di un *Cloud based security broker*, strumento che permette di controllare i dispositivi personali che possono accedere ai dati dell'organizzazione. Maggiori dettagli
nell'articol
o
https://www.ictsecuritymagazine.com/articoli/mitigare-rischi-sicurezza-nel-cloud-pubblico-cloud-access-security-brokers-casb/.

In parole molto povere, gli utenti devono “collegare” il proprio smartphone o tablet o pc al CASB dell’organizzazione per cui lavorano. In molti però fanno resistenza (curiosamente sono più propensi a fornire tutti i propri dati a OTT come Google, Amazon, Facebook e Apple che permettere al proprio datore di lavoro un controllo limitato del proprio dispositivo personale) e per questo è necessario pianificare attentamente l’introduzione degli strumenti CASB.

Le ISO/IEC 27001:2013 e ISO/IEC 27002:2013 non trattano del BYOD, anche se nel 2013 il fenomeno stava sempre più diffondendosi. È quindi necessario fare riferimento ad altre pratiche come per esempio le pubblicazioni SP 800-46 “Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security” e SP 800-114 “User's Guide to Telework and Bring Your Own Device (BYOD) Security” del NIST, anche se sono eccessivamente prolisse, o le linee guida del CESG, anche se complicate dalla suddivisione in più documenti.

Per chi vuole adottare la ISO/IEC 27001, come sopra suggerito è possibile aggiungere un controllo alla Dichiarazione di applicabilità o vedere il BYOD come caso particolare del già esistente controllo “A.06.02.01 Politica per i dispositivi portatili”.

Riflessioni finali

Le organizzazioni solitamente si nascondono le difficoltà nel controllare il BYOD. Infatti sono ben contente di aumentare la reperibilità del proprio personale, e di introdurre lo *smart working* a costi limitati. Quindi promuovono sempre più l’uso di strumenti cloud, anche se spesso si può accedere a questi con strumenti insicuri.

Ma oggi è anche necessaria una maggiore sicurezza e questo richiede di controllare in qualche modo la flessibilità e la libertà introdotta dalle nuove tecnologie.

Tali questioni non devono essere nascoste sotto il tappeto e vanno affrontate valutando correttamente tutti i rischi, tra i quali: le vulnerabilità introdotte, la possibilità di essere sanzionati per carenza di misure di sicurezza, personale meno connesso nel caso venga vietato il BYOD, persone scontente (o non sempre connesse ai sistemi dell’organizzazione) nel caso vengano introdotti strumenti CASB, maggiori costi per fornire al personale strumenti controllati dall’organizzazione.

A cura di: **Cesare Gallotti**