Un aggiornamento di Microsoft permetterà di sorvegliare i dipendenti

Un aggiornamento di Microsoft 365, a partire dal 2022, permetterà ai datori di lavoro di sapere qualsiasi cosa i dipendenti facciano con i dispositivi aziendali. Ogni azione sarà controllata, archiviata e analizzata e i trasgressori potranno essere facilmente individuabili. **Dimenticatevi che in futuro ci possano essere dei whistleblower (degli informatori) come Edward Snowden o Chelsea Manning** poiché ogni fuga di informazioni sensibili e di interesse pubblico sarà impedita.

Solo negli USA, ogni giorno, 730.000 tra aziende ed enti pubblici utilizzano il pacchetto di Microsoft 365 che vedrà inseriti, a seguito dell'aggiornamento, **strumenti di "gestione del rischio interno"**. Le organizzazioni che utilizzeranno questi nuovi strumenti potranno avere una "maggiore visibilità sui browser" di ciò che lo staff sta facendo sui browser Web Microsoft Edge e Google Chrome, migliorando la loro capacità "di rilevare e agire sui segnali di esfiltrazione del browser", inclusi "file copiati nell'archiviazione cloud personale, file stampati su dispositivi locali o di rete, file trasferiti o copiati in una condivisione di rete e file copiati su dispositivi USB".

Non solo. Sempre dal prossimo anno, Microsoft metterà a disposizione dei propri clienti anche dei bot di apprendimento automatico da inserire nei dispositivi aziendali col fine monitorare ogni azione dei dipendenti e segnalare ciò che viene ritenuto "rischioso"; **l'archiviazione, la gestione e l'analisi dell'insieme dei comportamenti del dipendente sui dispositivi elettronici verrà poi utilizzato per redigere un rapporto per ogni singolo dipendente**.

Tutto ciò che verrà fatto all'interno di un'organizzazione che utilizzi Microsoft 365 potrà quindi essere in mano al capo d'azienda, al capo d'ufficio oppure ai servizi segreti. Perché, oltre al profitto, Microsoft è interessata a tali dispositivi di sicurezza? I motivi sono due e interconnessi: tenere nascoste le proprie malefatte e compiacere il suo partner più importante, il Governo USA. Come riportato dal The Guardian nel 2013, Microsoft ha collaborato con l'intelligence statunitense per eludere la crittografia dei propri software al fine di permettere l'accesso alle chat dei dipendenti. Infatti, **il colosso dell'informatica di Bill Gates ha collaborato con la National Security Agency (NSA) e con l'FBI**, come a suo tempo rivelato da Edward Snowden. Ma in quei file ci sono anche le prove della più ampia portata della **collaborazione tra aziende della Silicon Valley e le agenzie governative di sicurezza e spionaggio**.

D'altronde, negli ultimi vent'anni, questi colossi della tecnologia e dell'informatica hanno accumulato contratti miliardari con le agenzie e i dipartimenti governativi statunitensi incaricati di sicurezza, spionaggio e guerra. Un rapporto prodotto negli Stati Uniti rivela che, fino ad oggi, **l'86% dei contratti governativi assegnati ad Amazon e il 77% di**

quelli assegnati a Google fino sono legati alla così detta "guerra al terrore". Delle cinque agenzie federali che hanno speso maggiormente acquistando dalle aziende tecnologiche negli ultimi due decenni, quattro sono: Dipartimenti della Difesa, Dipartimento della Sicurezza Nazionale, Dipartimento di Giustizia e Dipartimento di Stato; **dal 2004**, almeno **44,5 miliardi di dollari** sono passati da questo quartetto di dipartimenti **alle Big Tech della Silicon Valley**.

E il sistema delle porte girevoli agevola in maniera abnorme questi giganti che cooptano tra le proprie fila chi fino a poco tempo prima muoveva pezzi importanti del potere profondo e nascosto dello Stato. Ad esempio, è il caso di **Joseph D. Rozek**, con un passato di grande importanza presso il Dipartimento di Sicurezza, che adesso lavora per Microsoft come direttore esecutivo per la sicurezza interna e l'antiterrorismo dove è responsabile dello sviluppo e dell'implementazione di un piano aziendale strategico nell'area della sicurezza nazionale, dell'antiterrorismo e della condivisione delle informazioni. **Jared Cohen** ha invece lavorato al Dipartimento di Stato prima di passare a Google dove ha fondato Jigsaw, uno strumento antiterrorismo per piattaforme di social media che fino a poco tempo fa si concentravano esclusivamente su attori musulmani. **Steve Pandelides**, nell'FBI per oltre 20 anni – anche presso il National Counterterrorism Center e nella Operational Technology Division – è ora direttore della sicurezza di Amazon Web Services. **Nicholas Rasmussen**, già direttore del National Counterterrorism Center, adesso è direttore esecutivo del Global Internet Forum to Counter Terrorism fondato da Facebook, Microsoft, Twitter e YouTube.

La commistione tra le multinazionali tecnologiche e dell'informatica con il governo USA, e con altri governi in tutto il mondo, è ogni giorno che passa più invasiva e ciò che resta della democrazia diventa man mano sempre più intangibile, disgregata dai circuiti della gabbia digitale e dell'ossessiva volontà di potere e controllo di coloro che si riuniscono in consessi come il World Economic Forum.

[di Michele Manfrin]