La sicurezza informatica… sul lavoro

A ben guardare, lo scarsissimo livello di sicurezza dell'informatica contemporanea è riconducibile ad una singola causa: la scarsa comprensione dell'informatica da parte della popolazione. La pandemia ha notevolmente espanso la penetrazione dell'informatica nella società civile, ma questa penetrazione non è stata accompagnata da una maggiore comprensione del funzionamento dei software utilizzati.

Giacomo Tesio

Di sicurezza sul lavoro, sia essa informatica o fisica, in Italia si parla ancora solo a valle di incidenti eclatanti dagli esiti irreversibili, come avviene ancora troppo spesso, con la morte dei lavoratori. Periodicamente, casi come quelli di Luana D'Orazio o di Luisa Scapin, salgono agli onori delle cronache, scuotono l'opinione pubblica e generano splendide dichiarazioni di intenti fin dalle più alte cariche dello Stato… del tutto immemori delle vergognose tragedie precedenti, dalla Eternit alla ThyssenKrupp, passando per molte altre meno note.

Poi l'indignazione passa e tutto rimane più o meno come prima.

Tuttavia, l'indignazione che segue questi incidenti clamorosi è indicativa, se non di una cultura della sicurezza sul lavoro diffusa e radicata nella popolazione, quanto meno di una vaga comprensione del problema e della sua banale evitabilità: è chiaro, a valle di ogni incidente, che la salute delle vittime è stata sacrificata alla massimizzazione dei profitti aziendali ed alla riduzione dei costi; meno chiara è la natura probabilistica di tale sacrificio: la vittima non è stata esplicitamente scelta in anticipo, ma ha perso una drammatica roulette russa cui partecipa ogni lavoratore ed ogni lavoratrice che opera nelle medesime condizioni, rischiando gli stessi danni permanenti ed irreversibili, sebbene prevedibili e prevenibili.

La sicurezza informatica invece, in questo specifico momento storico, non gode ancora di questa pur vaga e limitata comprensione, capace di indignare le masse ed influenzare, anche solo superficialmente, l'agenda politica ed istituzionale.

In parte ciò è dovuto alla natura dei danni prodotti, molto meno evidenti per gli individui o per le aziende: di (in)sicurezza informatica si può morire, ma la riconduzione delle cause e delle responsabilità è molto più complessa. Vi è poi uno iato, una distanza fondamentale fra la definizione della sicurezza in ambito informatico e quella in ambito sociale e lavorativo, le cui conseguenze sono più subdole di quanto si immagini. Infine, la ragione fondamentale di questa differente percezione del problema risiede nella scarsa cultura informatica della cittadinanza e nella scarsa comprensione dei danni irreversibili che questa comporta.

La sicurezza informatica riguarda sempre e comunque l'accesso a dati.

Un dato è semplicemente una delle possibili rappresentazioni di un'informazione impressa su un supporto trasferibile ed interpretabile da un essere umano. L'informazione, spesso confusa con il dato stesso, è invece un'esperienza soggettiva di pensiero comunicabile nella mente di un essere umano. L'informazione esiste sempre e solo nella mente di un essere umano, effetto collaterale del vantaggio evolutivo offerto dal linguaggio, ma il dato, con l'invenzione della scrittura, della stampa e della rete, può veicolare un'informazione nello spazio e nel tempo.

L'informatica si occupa dell'informazione, di come questa possa essere trasferita, preservata, rappresentata, interpretata e trasformata, nonché delle tecniche che applicano tali conoscenze.

Potremmo dire che il dato sta all'informatica come la moneta sta all'economia o l'energia sta alla fisica: non ne esaurisce assolutamente l'essenza, ma è uno strumento fondamentale.

Caratteristica fondamentale del dato, è che la sua copia non lascia tracce.

Chiunque abbia accesso ad un dato può sempre copiarlo, diffonderlo o usarlo per i propri scopi e spesso può anche alterarlo sebbene nascondere le tracce di una alterazione sia più complesso.

Generalmente, quando si pensa alla sicurezza informatica, si pensa questa seconda tipologia di problemi legati ai dati, ai virus o ai ransomware, ovvero a software installati con l'inganno su computer bersaglio per danneggiarne i proprietari o richiedere un riscatto. Oppure si pensa agli "hacker", a criminali capaci di penetrare nei sistemi informatici governativi per manometterli, ignorando il fatto che in realtà le attività di cyberwarfare sono condotte da ingegneri che lavorano proprio per intelligence governative, mentre gli hacker, al massimo, portano alla luce vulnerabilità gravissime ed ampiamente sfruttate da criminali in precedenza, proprio per costringere i responsabili alla loro correzione.

La sicurezza informatica è infatti l'insieme di pratiche (alcune delle quali automatizzate o automatizzabili) che una organizzazione mette in atto per garantire che l'insieme degli utenti che hanno diritto di accedere ad un dato possa effettivamente esercitare tale accesso, mentre l'insieme complementare, costituito dagli utenti che non hanno tale diritto, non possa.

Per quanto semplice possa apparire questa definizione, le sue implicazioni sono largamente fraintese.

Anzitutto è importante notare in essa una riduzione tipica dell'informatica contemporanea: la persona viene considerata solo come utente, ovvero come utilizzatore di uno specifico programma ed i suoi "diritti" sono sia specificati che esercitati attraverso il software ed i suoi termini di utilizzo. Persino l'attaccante che sfrutta un errore di programmazione del software per ottenere accesso a dati cui non avrebbe diritto, è a tutti gli effetti, in termini informatici, un utente del software stesso.

La riduzione della persona da cittadino/lavoratore ad utente, porta con sé ulteriori implicazioni per nulla intuitive: ad esempio la stragrande maggioranza degli smartphone in commercio impediscono di fatto l'accesso degli utenti ai dati personali che questi emettono durante il proprio utilizzo,

garantendone invece l'accesso e l'accumulo alle società produttrici. Si tratta, ovviamente, di una cessione inconsapevole di diritti su quei dati che non è vietata dalla legge, ma che ha conseguenze talvolta eclatanti, come l'introduzione da parte di Apple (evitata solo grazie all'intervento di moltissimi esperti del settore) di sistemi di controllo automatizzato dei contenuti progettati per riportare alle autorità giudiziarie la presenza sugli iPhone di contenuti "vietati" da autorità preposte (a loro volta autorizzate da Apple) senza il consenso del proprietario.

Tuttavia va anche notato come non tutte le persone che interagiscono con un sistema informatico sono utenti. Ad esempio tutti coloro che vengono accidentalmente registrati da chi invoca assistenti virtuali come "OK Google" o che vengono accidentalmente ripresi da una videoconferenza con Google Meet, saranno automaticamente identificati e profilati, ma non costituiscono, di per sé, utenti del sistema: sono invece "data subject" i cui diritti sono teoricamente garantiti dalla Legge dello Stato (in recepimento del GDPR), ma che di fatto vengono ancora violati sistematicamente ed automaticamente in assenza di un sistema sanzionatorio efficace.

E' dunque evidente che il diritto alla protezione dei propri dati personali (impropriamente chiamata "privacy") è un tema legato alla sicurezza informatica, ma non sovrapposto ad essa: in termini di sicurezza informatica, l'utente di un iPhone o di un Android non deve avere accesso ai dati raccolti su di sé dal software in esecuzione sul proprio dispositivo, non deve essere in condizione di cancellarli, alterarli o impedirne la diffusione, mentre le diverse aziende che producono il software che tale utente utilizza, sì.

In un contesto lavorativo, è il datore di lavoro ad essere titolare del trattamento dei dati personali dei dipendenti, di cui deve garantire la sicurezza e la riservatezza. Ma come amministratore dell'azienda ha diritto di accedere (entro determinate condizioni) alle comunicazioni dei dipendenti veicolate dagli strumenti di lavoro (come email, messaggi privati su forum interni etc) con serie conseguenze sulla riservatezza delle comunicazioni sindacali e delle relazioni che ne derivano.

Non è un caso che il top management di Facebook, ad inizio 2020 discutesse di come realizzare e vendere un sistema di content control aziendale in grado di identificare, tracciare ed isolare automaticamente (attraverso una "AI") le discussioni dei dipendenti riguardo al concetto di "unionize".

Dunque un sistema informatico potrebbe paradossalmente essere perfettamente sicuro da un punto di vista formale ed al contempo danneggiare la vita della maggioranza delle persone che vi interagiscono.

La sicurezza informatica non si limita però ai dati personali, ma riguarda tutti i dati di una organizzazione. Da sempre i progetti di un prodotto innovativo sono l'obiettivo di attività di spionaggio industriale, ed in un'economia globale, tale pratica ha una scala planetaria.

Oggi tuttavia lo spionaggio industriale internazionale è estremamente facilitato dall'uso superficiale di strumenti informatici di terze parti: ad esempio, caricare i propri progetti "sul cloud", implica sempre renderli tecnicamente accessibili a terze parti, sottoponendo ad un rischio molto elevato gli investimenti in ricerca e sviluppo: poiché la copia dei dati non lascia tracce, ben oltre il 95% dei data breach non viene osservata per anni, rendendo difficile comprendere l'entità di questo rischio a coloro che non se ne occupano professionalmente.

Ad esempio, a fine 2020 negli Stati Uniti è stato scoperto un enorme data breach subito da agenzie federali, ministeri e migliaia di società in tutto il mondo, perpetrato grazie ad una serie di vulnerabilità nel software e nei sistemi cloud di tre aziende statunitensi: Microsoft, SolarWinds e VMware.

Gli attaccanti avevano avuto accesso (ufficialmente per mesi, più realisticamente per anni) ai documenti riservati ed alle email governative ed aziendali basate su Microsoft Office 365, incluse quelle di amministratori delegati o dei vertici dello stato, fra cui il Ministero della Difesa, il Ministero del Lavoro ed il Tesoro americano.

Ad inizio 2021, quattro vulnerabilità del software Microsoft Exchange hanno permesso l'accesso alla posta elettronica di oltre 250 mila organizzazioni in tutto il mondo, inclusi il Parlamento Norvegese e l'Autorità Bancaria Europea.

Poiché il software è esso stesso un dato, appare chiaro come la sua protezione è precondizione della sicurezza dei dati che elaborerà: ad esempio, nel già citato data breach del 2020, gli attaccanti avevano introdotto delle modifiche al sorgente dei software di SolarWinds per poter espandere il proprio attacco ai numerosi clienti di questa azienda.

Tuttavia, con la diffusione di sistemi robotici automatizzati, la sicurezza del software sta acquisendo rapidamente notevoli implicazioni sulla sicurezza e la salute pubblica: ad esempio un robot industriale o un veicolo pilotato automaticamente da un software (impropriamente detto "AI") può facilmente causare incidenti mortali sia a causa di errori di programmazione che a causa di manomissioni volontarie del software.

Emblematica, a questo riguardo, è stata l'uccisione di Elaine Herzbert da parte di un'auto a guida autonoma di Uber, avvenuta a Temple, in Arizona nel marzo 2018.

Il veicolo, una Volvo XC90 di oltre due tonnellate, viaggiava a 65 chilometri orari sotto il controllo del "pilota automatico" che aveva registrato la presenza della vittima in tempo per effettuare una frenata di emergenza. Tuttavia gli ingegneri di Uber hanno spiegato alla polizia di Temple che tale software era stato configurato per disabilitare le frenate di emergenza durante la guida autonoma "per evitare un comportamento erratico del mezzo" che avrebbe causato il mal d'auto ai clienti.

La responsabilità dell'incidente è stata scaricata però sulla dipendente di Uber a bordo del veicolo, Rafaela Vasquez, sebbene fosse stata lei stessa in pericolo e nonostante il fatto che le distrazioni dei passeggeri del veicolo durante la guida autonoma fossero ben note e studiate da tempo nell'azienda.

La disabilitazione della frenata di emergenza era stata effettuata da personale autorizzato, ovvero in modo informaticamente sicuro. Il passeggero non avrebbe potuto riabilitarla, proprio a causa delle policy di sicurezza informatica del software stesso. Tuttavia la sicurezza fisica del lavoratore stesso (nonché la sua libertà personale) è stata ridotta da coloro che detenevano tali diritti.

Più recentemente, alcuni server macedoni utilizzati per la firma crittografica dei Green Pass sono rimasti per mesi accessibili via internet con credenziali predefinite, permettendo a chiunque fosse a conoscenza del loro indirizzo IP di produrre certificati completamente falsi, ma riconosciuti come validi dalle tutte le App di verifica europee.

In questo caso, la sicurezza informatica del sistema era letteralmente inesistente: gli attaccanti non hanno dovuto adottare alcuna tecnica avanzata per accedere al servizio di firma dei Green Pass, e avrebbero potuto continuare a lucrare sulla loro vendita per anni se uno o più hacker non avessero messo in circolazione documenti palesemente falsi, intestati ad Adolf Hitler, Mickey Mouse e Bettino Craxi, per far emergere il problema.

I Green Pass palesemente falsi sono stati fra gli ultimi ad essere emessi da quel server, ma non sappiamo quante migliaia di altri Green Pass falsi siano stati emessi prima: appare dunque evidente che la sicurezza (o l'insicurezza) informatica di un sistema può avere notevoli conseguenze sulla vita e sulla salute dei cittadini e dei lavoratori, nonché sull'economia di intere nazioni e sulla credibilità della politica.

Ma come garantirla?

A ben guardare, lo scarsissimo livello di sicurezza dell'informatica contemporanea è riconducibile ad una singola causa: la scarsa comprensione dell'informatica da parte della popolazione.

La pandemia ha notevolmente espanso la penetrazione dell'informatica nella società civile, ma questa penetrazione non è stata accompagnata da una maggiore comprensione del funzionamento dei software utilizzati.

Da decenni, il mercato del software si concentra a ridurre al minimo lo sforzo cognitivo necessario ad utilizzare un software. "Don't make me think" è il titolo di una pietra miliare nella progettazione delle interfacce utente. La facilità di utilizzo di un software permette infatti di ampliare il suo mercato potenziale e, nel lungo periodo, massimizzare i profitti che derivano.

Con lo sforzo cognitivo, però, sparisce anche la consapevolezza e la coscienza critica.

Ma se è vero che è possibile utilizzare un software senza comprenderne il funzionamento, è altrettanto vero che non è possibile utilizzarlo in modo sicuro. Infatti, alla facilità d'uso si affianca spesso una straordinaria complessità interna, talvolta accidentale, talvolta scientemente perseguita dai produttori.

È certamente possibile insegnare agli utenti basilari pratiche di sicurezza informatica, ma senza una comprensione profonda del funzionamento del software cui vengono applicate, tale formazione può solo servire a scaricare la responsabilità degli inevitabili incidenti sugli utenti stessi.

Una catena infatti è solida quanto il più debole dei suoi anelli: senza una comprensione approfondita dell'informatica da parte di tutti i lavoratori che vi interagiscono, è impossibile garantire la sicurezza di un sistema cibernetico complesso.

Ed anche i pochi che riuscissero a memorizzare ed applicare correttamente tutte le pratiche necessarie nei diversi contesti di operativi di tale sistema, non avrebbero alcuna voce in capitolo rispetto alla scelta di software sicuri: se Rafaela Vasquez avesse compreso il funzionamento del programma alla guida del veicolo che ha ucciso Elaine Herzbert, non avrebbe accettato di salire a bordo per fare da capro espiatorio dopo la prima vittima. Analogamente, qualsiasi proprietario di un cellulare Android o qualsiasi utente di un browser come Google Chrome non ha idea dei rischi e delle conseguenze individuali e sociali di queste scelte "informaticamente sicure".

Di questa ignoranza diffusa le aziende approfittano sistematicamente: scrivere software sicuro significa scrivere software più costoso, per cui

l’azienda che rischia di più e massimizza i profitti (a discapito dei propri utenti) è quella che si può comprare i rari concorrenti virtuosi.

Infatti, in un contesto in cui la domanda non ha alcun modo di comprendere una vasta categoria di rischi connessi ad una certa categoria di prodotti, il mercato avvantaggia sempre i prodotti peggiori.

Il primo passo per garantire la sicurezza informatica sul lavoro è dunque insegnare informatica ai lavoratori. Attenzione: non insegnare ad usare un software da ufficio piuttosto che un altro, ma insegnare come questi software funzionano, ad analizzare come sono stati scritti, quali errori contengono, come potrebbero essere abusati e da chi.

Non c’è un modo più facile o rapido: solo comprendendo il funzionamento degli automatismi informatici che ci circondano, possiamo sceglierli ed usarli in modo sicuro per noi e per gli altri.

È un percorso difficile, ma sempre più urgente.