Cybersecurity alla sfida cognitivista, ecco i bias che ci rendono "insicuri digitali"

Percezione del rischio e attitudine mentale giocano un ruolo centrale nella capacità di proteggere i nostri dati personali. Portandoci spesso a sottostimare l'impatto di eventi avversi. Analizziamo le dinamiche che si celano dietro le quinte dei processi decisionali. E come superare gli ostacoli

La **cybersecurity** passa anche da una maggiore consapevolezza dei nostri processi decisionali. Per questo serve non solo una forte spinta strategica sull'alfabetizzazione digitale, ma anche una svolta etica nella fase di progettazione delle piattaforme online.

Un esempio su tutti, per capire di cosa stiamo parlando: tutti noi ricordiamo che perfino la password dell'**account Twitter di Donald Trump** – prima che questo venisse sospeso in seguito

ai fatti di Washington – era finita su tutti i giornali: **maga2020**. L'aveva individuata l'hacker "etico" Victor Gevers in soli cinque tentativi.

Partendo dallo slogan che ha accompagnato per anni il presidente, "Make America Great Again (usato spesso, appunto, con l'acronimo MAGA), il ricercatore olandese – fondatore della organizzazione non profit **GDI Foundation** – ha utilizzato questa violazione come simbolo delle **vulnerabilità della rete**, al fine di accrescere la consapevolezza degli utenti sui rischi di un uso non attento ai temi di sicurezza. Possiamo ridere del Presidente e del suo staff, ma ad essere sinceri la maggior parte di noi non **è tanto più attenta:** tra le password più usate in rete troviamo la stringa di numeri "123456", seguita da "123456789" e, subito dopo, l'immancabile "qwerty". Inutile sottolineare che sono anche le più facili da hackerare.

Per giunta **usiamo le stesse password per diversi account e dispositivi,** anche quando li condividiamo con amici e parenti, con un **comportamento estremamente rischioso**; è noto quanto le persone utilizzino password identiche per più domini (dal 40% fino ad un 80-90% in casi di parziale riutilizzo), per cui, nell'uso promiscuo di applicazioni apparentemente innocue – come **Netflix o altri account di video streaming tra amici** – c'è una implicita condivisione di dati sensibili, perché potenzialmente si stanno condividendo le medesime password utilizzate per account più impegnativi (**come ad esempio gli accessi bancari**).

Gli esempi di tutti quei piccoli incauti gesti che compiamo senza considerarli particolarmente insicuri, coinvolgono attività che sono entrate a pieno titolo nelle nostre abitudini e **facciamo fatica a immaginare possano essere rischiose**: dal lasciare che **Alexa** ci aiuti nelle attività domestiche, senza disabilitare la registrazione delle nostra conversazioni, fino all'invio di foto private, foto di bambini o foto intime, tramite Whatsapp e Facebook. Potremmo

continuare a lungo elencando piccoli comportamenti che mettiamo in atto **senza pensare troppo alle conseguenze in termini di cybersecurity** e viene naturale chiedersi quale sia effettivamente la base delle nostre scelte in termini di **sicurezza digitale**.

Percezione del rischio e bias cognitivi

Un discorso noto agli addetti ai lavori, che si fa sempre più urgente ed importante a livello globale anche per i non esperti, oggi che – per via dell'emergenza sanitaria – all'intera società è richiesto di intensificare l'uso del digitale tra **smart working**, **Dad** e **digitalizzazione della PA**.

Il **rischio** è definibile come la probabilità di subire un fatto negativo a fronte di variabili date, per cui nella nostra mente si traduce in un rapporto costi/benefici strettamente correlato al modo in cui percepiamo ed analizziamo la situazione pericolosa. Già nel 1738 Bernoulli aveva teorizzato l'**approccio psicofisico al processo decisionale**, sottolineando l'avversità al rischio: **la maggioranza delle persone preferisce una sicurezza minore a un azzardo incerto**.

L'avversità o la propensione al rischio, intesi come la possibilità di rifiutare o accettare un rischio futuro contro una sicurezza immediata, sono correlate essenzialmente non già ai risultati attesi, ma all'attesa del valore soggettivo dei risultati che si prevedono.

Il principio fondamentale sotteso al processo attribuzionale, prevede erroneamente che l'uomo sia in grado di padroneggiare la realtà, mosso da un bisogno fondamentale di **prevedere il futuro** e **controllare gli eventi.** Abbiamo bisogno di risposte confortanti anche nel confrontarci con la casualità, e tendiamo ad attribuire un significato a una struttura da noi percepita, specialmente quando il significato può essere confortante e ridurre l'instabilità dell'ignoto. **Ad esempio, la familiarità con una persona ci farà percepire le nostra**

interazioni digitali più sicure di quanto non lo siano: scambieremo dati e foto tramite whatsapp o email senza concepire il mio comportamento come pericoloso. Allo stesso modo, **gli ambienti dotati di determinate caratteristiche saranno correlati ad una elevata percezione di sicurezza** e saranno navigati senza troppe preoccupazioni.

In questo caso, intervengono le **quattro dimensioni fondamentali connesse alla sicurezza in ambienti digitali**, su cui convergono la maggior parte degli studiosi:

- **riservatezza**
- **integrità** delle informazioni scambiate
- **disponibilità** dei contenuti ricercati
- **non-repudiation** (non sconfessione) delle transazioni avvenute (soprattutto per i sistemi che prevedono pagamenti).

La teoria del doppio processo

La realtà è complessa, i soggetti sono molto poco razionali e gli esiti dei processi decisionali rispondono più alla necessità di sintesi e semplificazione che non da analisi causali e razionali. **Ciascuno di noi ha una sua personale attribuzione di pericolo alle situazioni a prescindere dalla loro reale ed oggettiva rischiosità**: le persone associano rischi differenti ad attività che essenzialmente hanno uguali probabilità di produrre conseguenze negative. Da questo punto di vista **il decision making essenzialmente si concentra sul concetto di percezione**, che **prescinde dal rischio oggettivo** ma si basa su giudizi e valutazioni che ne danno i soggetti.

Per comprendere i pregiudizi che guidano il nostro comportamento nell'analisi di rischio, è utile **ricondurre il pensiero umano in una struttura, chiamata "teoria del doppio processo"** che divide la cognizione umana in due modalità: una **implicita**, sintetica e veloce, che è anche quella più utilizzata nonostante ci faccia incorrere in errori, i bias

cognitivi; un’altra **esplicita**, lenta e sistematica, che sopraggiunge quando siamo disposti ad investire più energie.

Un dato ormai consolidato in letteratura è la **discrepanza tra la percezione soggettiva del rischio e la sua valutazione oggettiva**. Il **sistema di pensiero intuitivo** che agisce in modo preminente, seppur implicito, nel creare le nostre valutazioni coscienti, coinvolge le **reazioni emotive** che associamo a diversi stimoli. Per quanto incidano fattori individuali, ad oggi sappiamo che è possibile focalizzare la risposta ad una situazione di rischio principalmente attorno alla **percezione di gravità e probabilità di accadimento** di evento.

I **due criteri di classificazione** noti come **rischio terrificante e rischio sconosciuto**, sono intrinsecamente correlati alla componente affettiva che investe la situazione. Da una parte, quindi abbiamo la **percezione di conseguenze gravi**, correlata ad una certa attività e dall’altra la **possibilità che l’esito non si realizzi**, grazie alla capacità di controllare il possibile esito rischioso.

Partendo da questi due fattori ciascuno costruisce implicitamente una **personale mappa cognitiva della rischiosità** associata ad una determinata attività, che coinvolgerà anche la risposta emotiva connessa ai possibili esiti della situazione. In tal senso, **se le attività sono percepite come piacevoli e fonte di benefici**, come può ad esempio esserlo condividere foto personali con gli amici attraverso Whatsapp e Messenger, vengono considerate anche poco rischiose o per lo meno **la valutazione in termini di costi/benefici è sbilanciata a favore del beneficio** correlato alla condivisione, contro un costo che viene percepito come limitato e meno grave, anche in contraddizione con la logica fattuale.

Assunzione di responsabilità e processi

decisionali

Nella **cybersecurity** la comprensione ed il superamento della percezione relativa alla sicurezza, con i relativi bias decisionali, sono aspetti fondamentali, poiché influiscono sull'allocazione delle risorse e sull'analisi delle minacce. Il problema principale è che noi, in qualità di **"avari cognitivi"**, per prendere le nostre decisioni ci basiamo unicamente su quello che vediamo in modo rapido e tutt'altro che sistematico, senza realmente considerare tutte le informazioni a disposizione: **protagoniste del processo sono senza dubbio le euristiche**, le scorciatoie cognitive che agiscono a livello inconsapevole, che assumono un peso fondamentale nelle decisioni connesse alla valutazione del rischio, **lasciando un ampio margine di influenza alle emozioni correlate alle decisioni.**

La **componente del rischio** spesso non è basata quindi su un dato oggettivo, ma piuttosto sulla **percezione soggettiva** che ciascuno ha rispetto alla possibilità che un evento negativo si verifichi, ma soprattutto il peso emotivo che attribuisce alle opzioni immaginate.

Un ruolo più importante lo assumono, quindi, le **rappresentazioni che ciascuno costruisce, nel tempo ed in virtù di esperienze e relazioni personali**, le quali influenzano in maniera determinante i **processi decisionali.** Così accade che – in assenza di un pericolo imminente e conclamato – **le aziende preferiscano non chiamare un esperto di cybersecurity** o le persone evitino di aggiornare il costoso **antivirus** o ancora che non si impegnino a **cambiare effettivamente la password con costanza**, tutto questo pur di non spendere soldi o tempo hic et nunc.

Senza dubbio il frame e la comunicazione acquistano un rilievo non indifferente nel contesto, se pensiamo che, a parità di probabilità, cambiando la prospettiva del problema – ad esempio invertendo vincite e perdite – si nota una modifica

delle risposte (Prospect Theory).

Cybersecurity e effetto framing

L'effetto framing affida un peso rilevante al modo in cui viene contestualizzata la situazione in termini informativi: le parole che scegliamo per proporre un problema inficiano sul modo in cui leggiamo la situazione.

Facciamo un esempio:

- i dati Coware ci dicono che il 30% dei casi di ransomware include una minaccia di rilascio di dati esfiltrati ed il 22% contiene effettivamente questi dati.
- i dati Coware ci dicono che il 70% dei casi di ransomware non include minaccia di dati esfiltrati difatti solo il 22% contiene effettivamente questi dati.

L'informazione è esattamente la stessa, ma ad un lettore inesperto nel primo caso appare piuttosto allarmante, nel secondo tutto sommato rassicurante: **cambierà totalmente la mia percezione della pericolosità dei ransomware e le relative azioni di difesa che metterò in atto.**

In generale il negativo vince sul positivo, nella misura in cui il cervello risponde in fretta anche a minacce puramente simboliche, soprattutto se espresse in maniera emotivamente carica, arrivando ad **elaborare in maniera più sistematica le informazioni cattive rispetto a quelle positive**.

Oltre a questo, Kahneman ci ha dimostrato che le persone sono più propense a correre il rischio di una grossa perdita differita nel tempo, piuttosto che accettare nell'immediato una perdita reale più piccola, incorrendo così nel **bias del presente** (o hyperbolic discounting). Le ragioni di questa distorsione sono correlate ad un altro errore molto diffuso, che è la tendenza ad ignorare o sottostimare la possibilità che eventi negativi possano riguardarci in prima persona (**bias**

dell'ottimismo). Questo pregiudizio, **secondo la neurologa Tali Sharot**, ha una sua funzionalità adattiva: "Research on the optimism bias suggests an important divergence from classic approaches to understanding mind and behaviour. It highlights the possibility that the mind has evolved learning mechanisms to mis-predict future occurrences, as in some cases they lead to better outcomes than do unbiased beliefs".

Impatti del "bias dell'ottimismo"

Rispetto a credenze imparziali, la tendenza a **sovrastimare la possibilità di esiti positivi in futuro**, porta a risultati migliori, ed è un comportamento che si è andato consolidando, non solo per il noto processo di **minimizzazione delle perdite e massimizzazione dei risultati**, ma per una ragione ben più profonda: **il nostro sistema cognitivo elabora mappe del futuro tendenzialmente positive**, ancorandosi al presente e distorcendo i fatti in modo da non soccombere alla depressione o allo stress. **L'illusione ottimistica è quindi evoluzionisticamente necessaria**, andandosi a consolidare come processo più frequente nelle valutazioni quotidiane del rischio.

Per quanto alcuni autori arrivino a considerare le **illusioni ottimistiche come l'unico gruppo di miscredenze effettivamente adattive**, è necessario sottolineare che, in quanto **distorsioni cognitive**, si tratta sempre e comunque di un **processo potenzialmente pericoloso**, giacché la sottovalutazione del rischio può ridurre il comportamento precauzionale. Banalmente, **se riteniamo improbabile un attacco hacker al nostro sistema informatico, procrastineremo monitoraggi, controlli ed aggiornamenti facendoci trovare vulnerabili nel caso di incursione.**

Allo stesso tempo si attiva il **pregiudizio egoistico** per cui **il soggetto attribuisce la "colpa" di ciò che gli accade in prima persona a fattori ambientali o contestuali** piuttosto che interiorizzare l'errore come un tratto interno. In caso di

attacco, quindi, saremo portati a sminuire le nostre responsabilità **attribuendo al virus, all'hacker o al sistema vulnerabile**, una potenza superiore alle possibili attese. Come attori sociali, abbiamo la consuetudine di osservare il mondo dal nostro personalissimo punto di vista, il che attiva in modo più vivido un pregiudizio che è frequente nel nostro funzionamento cognitivo: l'**errore fondamentale di attribuzione**. Si tratta della tendenza a vedere i fallimenti o gli errori di altre persone come parte della loro identità invece che attribuire il fallimento o l'errore a influenze contestuali o ambientali.

Questo accade in maniera ancora più sistematica se abbiamo un'elevata sensazione di **controllo personale del rischio**, perché l'idea di avere capacità per gestire la situazione ci fa percepire meno grave il pericolo, soprattutto se ci siamo esposti volontariamente alla situazione rischiosa. A questo è associato il **bias di conferma** che porta ciascuno ad essere d'accordo con le persone che la pensano allo stesso modo ed evitare individui o gruppi che la pensano diversamente ed inducono disagio o dissonanza. **Il bias di conferma** non solo influenza le nostre strategie di ragionamento, ma **influisce anche sul modo in cui memorizziamo le informazioni e le recuperiamo quando necessario**. Le persone tendono a concentrarsi e ricordare le informazioni che confermano o si allineano con le loro convinzioni, mentre **scartano o dimenticano le informazioni che si oppongono al loro punto di vista**.

Anche gli esperti, ad esempio, potrebbero incorrere in questo pregiudizio inconsapevolmente, trovandosi a cercare soluzioni a problemi associati ad un evento avverso, solo fra le cause in linea con le proprie teorie. IIl superamento del bias di conferma richiede un pensiero creativo e flessibile, in particolare il capacità e volontà di guardare una situazione da diversi punti di vista.

Sfida etica per i progettisti

Preso atto che, spesso, **il nostro sistema cognitivo incorre in errori e distorsioni**, è ancora più chiaro quanto la percezione del rischio sia un processo personale e complesso, nel quale la **relazione tra rischi e benefici** di un'attività o di una situazione siano percepiti in modo differente da come questa relazione si realizzi nella realtà. **Dato oggettivo e percezione soggettiva non coincidono**, ma **questa consapevolezza va resa parte della cultura digitale** e dei suoi processi di **alfabetizzazione**.

Nel momento in cui si spinge verso una maggiore utilizzo del digitale, **l'insicurezza digitale diviene ancora di più un problema pubblico ed urgente.** Quotidianamente noi consegniamo ai gestori delle piattaforme importanti informazioni personali, per cui assieme alla **sensibilizzazione civica** rispetto al problema, si pone anche una **questione etica dei progettisti**, cui corre l'obbligo di implementare sistemi che prendano atto delle nostre debolezze cognitive, non per sfruttarle a proprio vantaggio, ma per aumentare la sicurezza della navigazione dei propri utenti.

Come sempre, le competenze tecniche e l'uso dei mezzi hanno scarso effetto se non dialogano con le competenze immateriali e culturali di sensibilizzazione rispetto agli effetti a lungo termine di azioni concrete. **L'attuale cyber-insicurezza** dipende senza dubbio "**dall'evoluzione rapidissima degli attori**, delle modalità, della pervasività e dell'efficacia degli attacchi", ma dobbiamo necessariamente contemplare la componente umana, le scelte personali, le "credenze" ed i comportamenti dei singoli. In tal senso le abitudini e l'educazione connesse alla sicurezza acquistano un peso decisivo nel discorso pubblico.