CyberMSME

Cybersecurity per Micro, Piccole e Medie Imprese

Approccio human-centered vs. Priorità aziendali — line guida

By CTS Customized Training Solutions & CASE

Erasmus+

Obiettivi e risultati:

Alla fine del modulo sarai in grado di:

- Definire e riconoscere l’approccio human-centered
- Cercare cos’è più importante tra l’approccio human-centered e le priorità aziendali
- Utilizzare l’approccio human-centered nel piano di gestione della cybersecurity
- Creare e definire un programma bug bounty

Index

Unità 1: Approccio human-centered

Sezione 1.1: Che cos'è l'approccio human-centered?
Sezione 1.2: Come utilizzare l'approccio human-centered nel piano di gestione cybersecurity

Unità 2: Bug bounty

Sezione 2.1: Che cos'è un bug bounty?
- Perchè creare un programma bug bounty? E quando farlo?
- Come creare categorie di bugs e bounties rilevanti?

Sezione 2.2: Caso studio: A.S Watson Group è il più grande gruppo retail del settore salute e bellezza
Sezione 2.3: Quale insegnamento possiamo trarre?
Sezione 2.4: Che domande porsi prima di attuare un programma bug bounty?
Sezione 2.5: Lasciati ispirare!

Unità 1: Aprroccio human-centered

Sezione 1.1: Che cos'è l'approccio human-centered?

L'approccio human-centered è un modo creativo di fare problem-solving.
È un processo che mette al centro i bisogni, le esperienze, i pensieri e le credenze delle persone per cui stiamo progettando il nostro prodotto.

In questo tipo di approccio, consideriamo l'audience l'insieme dei nostri utilizzatori.
Tale processo culmina con la creazione di una soluzione customizzata sulla base dei bisogni, esperienze e comportamenti del ricevente.

Questo è possibile focalizzando l'attenzione sul cliente e facendo leva sull'empatia, sull'ascolto attivo e sull'ideazione di molti prototipi.

Relevant links: Ideo > **Tools** (https://www.ideo.org/tools);
Design Kit > **What is Human-Centered Design?** (https://www.designkit.org/human-centered-design)

L’approccio human-centered si suddivide in tre fasi:

L’Ispirazione

In questa fase sono fondamentali le ricerche di mercato per capire quali sono i bisogni degli utilizzatori.

L’Ideazione

In questa fase, sulla base delle informazioni raccolte, si sviluppano i primi prototipi.

L’Implementazione

In questa fase, si procede a testare i prototipi messi a punto.

Erasmus+

Come sapere se effettivamente la soluzione è umanocetrica?

Se l'utilizzatore finale è sempre stato messo al centro del processo di creazione per cercare di capire quali erano i bisogni da soddisfare, la soluzione è umanocentrica!

E per quanto riguarda le priorità aziendali?

Dopo tutto, ciascuna azienda ha le proprie priorità, e non sempre coincidono con quelle dell'utilizzatore finale.
Qual è il motive per cui porti avanti l'attività?
Desideri una vita stabile, dei buoni profitti o stai perseguendo un sogno?
Qualsiasi sia il motive, non c'è nulla di sbagliato nel mettere al primo posto le priorità dell'azienda e del team piuttosto che l'utilizzatore finale.

Erasmus+

Quindi...l'approccio human-centered è un'utopia?

No. Oggi per avere successo è essenziale porre al centro l'utilizzatore, e l'approccio human-centered è un metodo molto efficace per riuscirci! Portare avanti un'attività, infatti, non è una scelta tra "me o loro".

Ti stai domando, allora, cosa sia più importante?

Dunque, non c'è una risposta giusta.

Senza gli utilizzatori, non c'è l'azienda. Senza l'azienda, non ci sono i prodotti, i servizi e gli utilizzatori.

Quindi, è importante trovare un equilibrio e tenere conto, anche, delle tue esigenze.
Nelle sezioni che seguono, capirai come utilizzare un approccio human-centered in un contesto di cybersecurity senza compromettere le priorità aziendali

Sezione 1.2. Come utilizzare l’approccio human-centered nel piano di gestione cybersecurity?

Come abbiamo detto, la chiave per far sì che l’approccio human-centered sia efficace è empatizzare con gli utilizzatori. Le persone hanno bisogno di sapere che ti stai prendendo cura di loro e stai considerando i loro valori. Pensiamo un attimo a quali sono questi valori...

Tutti gli utenti vogliono sentirsi al sicuro quando navigano su internet, questo vale soprattutto nel post-pandemia, in quanto sempre più persone che prima non lo facevano hanno iniziato a lavorare ed acquistare online.

Perciò, quello che devi fare è creare siti, piattaforme, software sicuri. Prima riuscirai a trovare tutti i bugs, prima potrai iniziare ad utilizzare un approccio human-centered.

Dove iniziare?

Usa il modello del programma bug bounty.

Unità 2: Bug bounty

Sezione 2.1. Che cos’è un bug bounty?

Molte aziende, organizzazioni e sviluppatori offrono un programma bug bounty, il quale permette all’utente finale di riconoscere i bugs (specialmente quelli concernenti lo sfruttamento delle vulnerabilità) e farlo sapere immediatamente all’admin.

Questo tipo di programma aiuta le aziende a testare i loro prodotti in modo più accurato. Infatti, pur se l’azienda assumesse personale per controllare la qualità dei prodotti, non riuscirebbe a verificare ogni dettaglio prima del lancio. Fare più test significa scoprire e risolvere i bugs più efficientemente e prevenire abusi e hackeraggi.

Erasmus+

Perchè creare un programma bug bounty? Quando farlo?

Se hai intenzione di lanciare un prodotto online, un sito o un software, dovresti pensare di creare un programma bug bounty.

Certamente, si consiglia di utilizzare questo tipo di programma in modo supplementare ad altri tipi di assicurazione sulla qualità stipulate prima del lancio.

Tuttavia, poche persone non possono trovare qualsiasi problema in poco tempo e assumere un B2B specialist potrebbe comportare dei costi aggiuntivi. Creando un programma bug bounty ottimizzerai il tempo e i costi!

Per far funzionare un programma bug bounty hai bisogno di definire:

- Categorie di bugs da identificare
- Un bounty rilevante
- Canali di comunicazione a cui inviare i report
- Una policy bounty

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Come creare categorie di bugs e bounties rilevanti?

Non c’è un unico metodo per creare categorie di bugs e assegnare I bounties. Tutto dipende dale caratteristiche del prodotto, del sito web, del software e dai contenuti.
Dai un’occhiata al seguente caso studio

Sezione 2.2. Caso studio: A.S. Watson Group è il più grande gruppo retail nel settore salute e bellezza

Website: **www.aswatson.com**

A.S. Watson aprì un programma bug bounty a luglio 2020. L’obiettivo era quello di rendere sicuro il sito del gruppo retail più grande al mondo nel settore salute e bellezza .

A.S. Watson Group ha postato informazioni sul programma sul sito **HackerOne**:
https://hackerone.com/watson_group?type=team&view_policy=true

Erasmus+

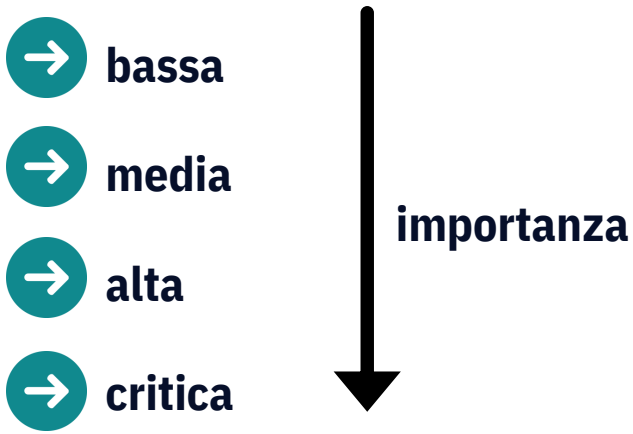
Il modello operative di A.S. Watson Group

Stabilire delle categorie di prodotto

L'azienda suddivise sia il sito web che l'app in due categorie. Successivamente, quale delle due dovesse avere la priorità.

Stabilire categorie di bugs

Non tutti i bugs hanno la stessa rilevanza, perciò è importate stabilire chiaramente quale categoria deve avere la priorità. Ecco l'esempio di gruppo A.S. Watson Group:



Erasmus+

Stabilire bounties

A.S. Watson Group fornisce ricompense per i due diversi prodotti a seconda della categoria di bug.

L'importo per bug è $100-4000. Dai un'occhiata alla tabella:

	bassa	media	alta	critica
Prodotto categoria 1	$100	$500	$1 500	$4 000
Prodotto categoria 2	$100	$250	$1 000	$3 000

Sulla base di quanto riportato sul sito HackerOne, il programma bug bounty ha già portato alla risoluzione di 60 problem segnalati. L'import medio per bug riportato è $250.

Erasmus+

Stbilire i canali comunicativi e le regole

Il sito HackerOne è la piattafroma attraverso la quale l'azienda prende contatti con la comunità etica di hacking.
Perciò, il gruppo AS Watson non ha bisogno di stabilire quali canali comunicativi utilizzare, sono già incorporati nella piattaforma insieme ad altri strumenti: aggiornamenti, notifiche, ranking dei migliori hacks ecc..

Inoltre, la pagina informa anche i richiedenti di:

- Quanto tempo devono aspettare prima di ricevere una risposta
- Quanto tempo occorre
- Quanto tempo devono aspettare i richiedenti per sapere il prezzo
- Entro quanto tempo saranno applicati I miglioramenti

Erasmus+

Quali sono i vantaggi per l'azienda?

- Il modello operativo del Gruppo A.S Watson è semplice e trasparente, questo contribuisce al miglioramento della credibilità aziendale.
- L'azienda è in grado di testare il sito e l'app più spesso grazie all'aiuto di una community professionale.
- Grazie alla community, l'azienda è in grado di identificare un numero di bugs molto superiore.
- La creazione di differenti categorie di prodotto e di bugs, attira le persone orientate ai processi. Ottime recompense,invece, attraggone le persone orientate al risultato.
- Contenuti interessanti e prodotti innovative attirano le persone orientate alla creatività

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Cyber MSME

Quali sono i benefici di una hacking community etica?

- Gli haker fanno ciò che sono bravi a fare.
- Ricevono un corrispettivo.
- Si sentono motivati, se inclusi nei processi di miglioramento aziendali
- Contribuiscono ad incrementare la cybersecurity.
- Contribuiscono al miglioramento del sito e dell'app.
- Proteggono gli utenti da potenziali minacce.
- Possono creare il loro portfolio.

Sembr che nessuno abbia qualcosa da perdere.

Erasmus+

Sicuramente, il gruppo A.S. Watson si prende cura della cybersecurity attraverso il programma bug bounty. Dov'è l'approccio umanocentrico?

Il caso che abbiamo appena analizzato è un Perfetto esempio di bilanciamento tra approccio human-centered e priorità aziendali. Perchè? Analizziamolo insieme:

Quale dovrebbe essere la priorità più importante del gruppo?
Probabilmente una qualità migliore del sito e dell'app, profitti maggiori e un'audience più grande.

Che cosa ci guadagna l'azienda da una hacking community etica?
Un ambiente virtuale più sicuro per tutti.

Detto questo, qual è la priorità per l'azienda?
L'utilizzatore. Per questo possiamo affermare che utilizza un approccio human-centered

Sezione2.3. Quale insegnamento possiamo trarre?

- Per creare un nuovo prodotto/servizio, oggi è indispesabile che le aziende tengano conto dei bisogni e aspettative degli utilizzatori.
- Nel processo di creazione, utilizzare un approccio human-centered è molto utile.
- Un approccio human-centered, tuttavia, non deve surclassare le priorità aziendali.
- Le priorità e valori aziendali formano un'attività tanto quanto il suo pubblico.
- Attuare un programma bug bounty è il metodo migliore per trovare il giuto bilanciamento tra l'approccio humen-centered e le priorità aziendali
- Puoi implementare un programma bug bounty per migliorare il piano di gestione cybersecurity

Sezione 2.4. Che domande porsi prima di attuare un programma bug bounty?

- Cosa vuoi sottoporre a revision (sito web, parte del sito, online store, applicazioni, software, parti di software, etc.)?
- Se ci sono diversi prodotti da controllare: li categorizerai? Quali priorità darai alle categorie?
- Quali tipi di bugs avranno la priorità: bassa; media; alta; critica?
- Quali ricompense offrire per specifiche categorie di bugs ?
- Che tipo di metodo di segnalazione bug sceglierai? Userai una piattaforma specifica?

Erasmus+

Sezione 2.5. Lasciati ispirare

Non c'è un singolo metodo per creare un programma bug bounty, e non ci sono regole esatte per dare bounties o categorizare categorie.
Per questo motivo dovresti dare un'occhiata ai siti delle grandi compagnie che lo stanno già utilizzando come Aliexpress, Android, T-Mobile e Google

Ecco alcuni link da visitare:

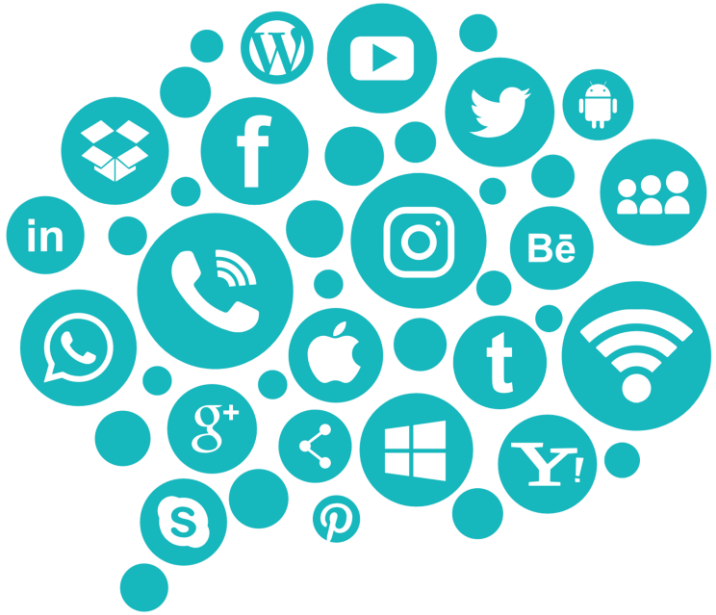
HackerOne: https://hackerone.com/bug-bounty-programs

BugCrowd: https://www.bugcrowd.com/bug-bounty-list/#accept

Buona fortuna!

Erasmus+

Grazie per l’attenzione!



The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.