STORMSHIELD

MEINUNGEN

DIE SCHLÜSSELROLLE VON UX IN DER CYBERSICHERHEIT

Julien Paffumi
Product Management Leader, Stormshield

Und wenn Cybersicherheit nicht mehr ein Zwang, sondern ein Reflex wäre? Um den Menschen zwischen Tastatur und Stuhl zu einem echten Garanten für digitale Hygiene zu machen, müssen die ihm zur Verfügung gestellten Werkzeuge Lust machen, sich mit ihnen zu beschäftigen. Mit UX haben Unternehmen in dieser Hinsicht einen Trumpf.

1993 ist die Geburtsstunde des Konzepts der „*User Experience*“, entwickelt von Don Norman, für den „*alle Aspekte der Erfahrung eines Individuums mit einem System berücksichtigt werden müssen*“. Der gesamte Ansatz hinter diesem Konzept besteht darin, dass die Benutzer sich ein Werkzeug zu eigen machen, sich dessen Besonderheiten aneignen und davon profitieren wollen. Diese „*User eXperience*“ (UX) lässt sich mittlerweile auf jeden Bereich anwenden und ist besonders für die digitalen Strategien von Unternehmen interessant. Im Dienste einer effizienten Cybersicherheit kann sich UX als echter Gewinn erweisen und die Verteidigungsposition eines Unternehmens sowie das digitale Vertrauen der Mitarbeiter stärken.

ZUR ERFOLGREICHEN CYBERSICHERHEIT GEHÖRT AUCH UX

UX ist nicht strikt dem sogenannten „Endanwender“ vorbehalten. Genauso wichtig ist die Annahme eines Sicherheitsprodukts durch einen Administrator. Es gibt also zwei Haupttypen von UX-Nutzern in der Cyberwelt: den technischen Nutzer (Administrator) und den Endnutzer. *„Es gibt Schnittstellen für Administratoren und Schnittstellen für Unternehmen. Ziel der UX ist es, dass sie in beiden Fällen von jedem genutzt werden können - indem sie für den durchschnittlichen Benutzer einfach und für den Experten komplex gehalten werden“*, erklärt **Sébastien Viou**, Cyber Evangelist Consultant bei Stormshield. Ein Administrator benötigt eine Sicherheitslösung mit einer guten UX, um die Verwaltung von Agenten in der IT-Umgebung, die Umsetzung von Sicherheitsrichtlinien oder die Überwachung von Ereignissen zu erleichtern. Kritischer Punkt auch bei der Cybersecurity: Eine gute UX hilft dem Administrator, mögliche Konfigurationsfehler in Sicherheitstools zu reduzieren - die sofort zu Schwachstellen für das Unternehmen werden. Was den Endbenutzer betrifft, so muss es die UX ermöglichen, sich ein Produkt leicht anzueignen, es zu verstehen und Lust zu haben, es zu benutzen, oder manchmal sogar einfach zu vergessen. Es ist daher notwendig, die Implementierung von Cybersicherheit durch UX zu fördern, wobei die Realität der dahinterstehenden Anwendungen berücksichtigt werden muss.

„Das Ziel von UX ist in beiden Fällen, dass sie für jeden nutzbar sind - und zwar so, dass sie für den durchschnittlichen Nutzer einfach und für den Experten komplexer sind“

Sébastien Viou, Stormshield Cyber-Evangelist Consultant

UX wird bei der Gestaltung von Cybersicherheitslösungen immer wichtiger. Und, wie **Guillaume Poupard,** Generaldirektor der ANSSI, bereits 2018 sagte: "*Wir müssen die digitale Sicherheit sexy, d.h. verständlich machen*". *„Man muss verstehen, was man sichern will, gegen welche Art von Bedrohung, mit welchen Mitteln und indem wir Leute einladen, die nicht Teil des Cybersecurity-Serails sind*“.

„Man muss die digitale Sicherheit sexy machen“

Guillaume Poupard, Generaldirektor der ANSSI

CYBER-BENUTZERFREUNDLICH: EIN HAUCH VON SEXY IN DEN IT-SICHERHEITSLÖSUNGEN

Cyberkultur und UX sind ein und dasselbe. Eine gut funktionierende Cyber-Kultur ist eine Kultur, die die Annahme von Sicherheitslösungen durch die Mitarbeiter aufgrund ihrer Sensibilität vorsieht. Anbieter müssen dies bei der Gestaltung ihrer Produkte berücksichtigen und sie mit einem betriebswirtschaftlichen und nicht nur einem technischen Ansatz entwickeln. Die Technik ist ein Hilfsmittel, aber was im Mittelpunkt von UX stehen muss, ist das Verständnis für das Alltagsgeschäft der Nutzer. Wie können wir also diese Produkte benutzerfreundlicher gestalten? Die Cyber-Community und die Hersteller arbeiten daran, und es gibt bereits viele Initiativen.

UX-Design-Sessions sind bereits entstanden und ermöglichen es den Herausgebern, ihre Lösungen bei Partnern und Kunden zu überprüfen. Das Ziel hinter diesem Ansatz ist es, ein Produkt während seiner Entwicklung neu auszurichten oder zu verfeinern, oder ein bestehendes Produkt weiterzuentwickeln, um eine effiziente und intuitive Handhabung zu gewährleisten. Diese Sessions sind dazu da, eine HCI zu entwickeln, die so nah wie möglich an der Tätigkeit und den Bedürfnissen der Benutzer ist. *„Bevor wir grafische Benutzeroberflächen für unsere Stormshield Data Security-Lösung entwickeln, entwickelt man Mockups, die man mit einer Gruppe von Benutzern testet"*, erklärt **Jocelyn Krystlik**, Business Unit Data Security Manager bei Stormshield. Die Idee ist es, Leute, *die Cybersecurity-Kunden sind, mit Leuten zu mischen, die keine sind, um die Anbieter herauszufordern"*.

Auch UX-Tests werden häufig eingesetzt. Dieses Verfahren zielt darauf ab, einen Benutzer in Echtzeit mit einer Lösung zu konfrontieren und seine Reaktion auf das Produkt zu analysieren. Dies hilft festzustellen, ob die Lösung intuitiv ist oder nicht, und sie ggf. anzupassen. Einige Herausgeber stellen auch kollaborative Plattformen zur Verfügung, auf denen ihre Kunden aufgefordert werden, Produkte zu testen und ihr Feedback und Bewertungen zu teilen. **Virginie Ragons**, UX/UI-Designerin bei Stormshield, erklärt: *„Sicherheitslösungen befinden sich in der Regel innerhalb komplexer Ökosysteme, und das Ziel ist es, den Anwendern eine harmonisierte interaktive Nutzung und eine intuitive Benutzeroberfläche zu bieten, damit sie ihr ursprüngliches Ziel erreichen können"*.

„Ziel ist es, den Anwendern eine harmonisierte interaktive Nutzung und eine intuitive Schnittstelle zu bieten, um das Erreichen des ursprünglichen Ziels zu erleichtern"

Virginie Ragons, UX/UI-Designerin bei Stormshield

Ein weiteres wichtiges Thema für Herausgeber bei UX: die Optimierung der Vorkonfiguration ihrer Lösungen. Das verfolgte Ziel? Die Schnittstellen sollen nicht mehr mit Optionen überladen werden, die man nicht benützt, und im Vorfeld muss unterschieden werden, was am meisten verwendet wird, und es dann in der Lösung voranzustellen. Dieser Schritt ist von entscheidender Bedeutung, denn die Art und Weise, wie die Redakteure eine Benutzeroberfläche gestalten, wird die Wahl der Benutzer bestimmen.

Der Herausgeber Kaspersky führt an, dass über 90 % der Sicherheitsvorfälle auf menschliches Versagen zurückzuführen seien. Genug, um uns sagen zu lassen, dass für eine erfolgreiche Cybersicherheit der Benutzer das letzte Wort bei der UX von Sicherheitsprodukten haben muss. Ein Anwender, der auch das letzte Wort in Sachen Trends zu haben scheint, mit wechselnden Nutzungsgewohnheiten und daher einem Design, das sich entsprechend weiterentwickeln muss, wie Sébastien Viou betont: *„Vor zwanzig Jahren ging es nur um die Steuerung. Dann kamen Sicherheitslösungen in Form von Heavy Clients, und jetzt geht der Trend zu Thin Clients mit ästhetischen Schnittstellen. UX folgt der globalen Evolution des Web"*.

CYBERSECURITY UND UX: DIE WICHTIGSTEN TRENDS

Die Entwicklung geht hin zu Thin Clients oder gar Arbeitsplätzen, die gar keinen Bearbeiter mehr haben, sie ermöglicht insbesondere die Anpassung an neue Nutzungsformen wie Nomadentum oder Demokratisierung der Telearbeit. *„Bei Stormshield haben wir dieses bearbeiterlose Konzept mit unserer Datenverschlüsselungslösung umgesetzt, die nun direkt im Browser genutzt werden kann. Dies wird in unserem Produkt Stormshield Data Security als bearbeiterlose Verschlüsselung bezeichnet*", sagt Jocelyn Krystlik. *Da Datenverschlüsselung ein wichtiges Thema ist, das eine Vielzahl von Personen in einem Unternehmen betrifft, ist es unerlässlich, die richtigen Werkzeuge zu haben, um diese Personen zu unterstützen und ihnen beizubringen, wie man damit umgeht.*"

Die Verantwortung der Mitarbeiter ist auch einer der wichtigsten Trends im Bereich UX. Der Endanwender wird zunehmend gefordert sein, für die Sicherheit innerhalb seiner Organisation zu sorgen. Das Konzept der Cybersicherheit erstreckt sich tendenziell auf alle Geschäftsbereiche, nicht nur auf technische Bereiche. Jeder Benutzer muss in der Lage sein, eine Rolle zu spielen. Auch hier wird UX zu einem wesentlichen Teil der digitalen Hygiene: man muss die richtigen Werkzeuge haben, um diesen Trend zu unterstützen. Für Administratoren beispielsweise muss UX effiziente und nachvollziehbare Mittel zum Sammeln und Melden der Informationen zur Verfügung stellen. Der Endanwender seinerseits muss in der Lage sein, Informationen zu übermitteln, insbesondere an die Administratoren. Sie profitieren sogar von einem größeren Anteil an sicherheitsrelevanten Entscheidungen, die nicht mehr nur den Technikern vorbehalten sind.

UX zeigt also viele Qualitäten und ist durchaus daran interessiert, in die Cybersecurity- und IT-Transformationsstrategien von Unternehmen integriert zu werden. Im Übrigen kommunizieren immer mehr Cybersicherheitsunternehmen über UX und seine Schlüsselrolle in ihren Produkten. Wie Hypori, das seiner Sicherheitslösung für mobile Geräte einen zweiten Schub gab dank UX. Oder auch die Firma Callsign, mit der Entwicklung einer Authentifizierungslösung komplett von und für die Anwender.

Interfaces mit einem vereinfachten und intuitiven Design, wenige Handgriffe für die Benutzer, angepasste Architekturen... UX? Zweifelsohne ein Cyber-Trend, dem man folgen sollte.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**