Human-centric Security Design Reduces Threats by Changing User Behavior

With widely differing motivations and behaviors, humans represent both the most important asset and the biggest risk factor in any security system. Consequently, a successful cyber security strategy must focus not just on the technical aspects, but also on the human element. This human-centric security design delivers more effective and efficient security solutions.

Human-centric Security Design Delivers Key Benefits

According to a recent report by IBM, 95 percent of cyber security breaches result from human error. When organizations design security around the human element, they reduce human vulnerabilities and mistakes that lead to breaches.

Addressing the human element means that security teams include employees in the security design process from the beginning. And when employees participate in the solution, they tend to trust and engage in the process more readily. This in turn increases employee compliance with security policies and best practices.

Finally, by avoiding unnecessary or ineffective security measures, human-centric security optimizes the use of resources and reduces costs. Security becomes a natural part of the workflow, rather than a hindrance, minimizing frustration and improving productivity.

Challenges to Address

While human-centric security delivers undeniable benefits, it does involve challenges. To begin with, security designers must acknowledge and embrace the diversity and complexity of their end users. They bring different backgrounds, skills, and roles to the table.

In addition, a single user may behave differently depending on the context. For example, employees may behave differently when working remotely than they do in the office. Likewise, nurses may need greater access to patient data when working on the ward than they do when they return to the office.

Another challenge of human-centered security design involves balancing security and usability. For instance, while enforcing strong passwords or multi-factor authentication (MFA) may improve security, it also increases user frustration. On the other hand, automating certain security tasks may improve usability but also introduce new vulnerabilities.

Successful Strategies Begin with Collaborative Process

No single security solution will fit all organizations or situations. Instead, effective strategies require a deep understanding of context and users. Smart security teams start with user research to determine how they work, their pain points in relation to security, their goals, and expectations. Observation, user interviews, and focus groups will prove useful tools.

Based on user research, security designers then define user requirements for the security solution. The resulting solution will balance user requirements with strategic goals, business needs, and regulatory compliance. To prove successful, it must provide adequate protection while remaining user-friendly, intuitive, and flexible.

Include end users in the security design process by soliciting feedback and involving them in usability testing. This helps to promote a mindset of shared responsibility for security. It also uncovers potential problems that would prevent widespread adoption of security policies.

Emphasize User Education

An essential aspect of human-centric security includes educating and empowering all end users. Targeted and engaging security awareness training programs increase user skills and confidence, making them an important first line of defense.

Effective training includes practical exercises, simulations, and feedback mechanisms to reinforce learning. Such training works best when geared toward specific user roles and responsibilities.

Additionally, organizations should establish clear reporting channels and procedures for employees to report incidents and suspicious activities. This way, organizations can foster a culture of trust and collaboration, as well as detect and contain threats faster.

Change User Behavior to Reduce Risk

eMazzanti cyber security experts understand that the best defense involves a layered security approach combined with education. Addressing user behavior and involving employees in the security process from the beginning minimizes risk while reducing downtime.

Consequently, eMazzanti designed MXINSPECT Security Awareness to help users recognize and reject business email compromise, phishing, and other cyber threats. By combining engaging, actionable training content with phishing simulations, MXINSPECT reduces successful attacks by up to 90 percent.