

Säkerhetshoten sätter design och lärande på sin spets



I dagens digitaliserade samhälle har teknologins inflytande förvandlat olika aspekter av människors liv, vilket medför både stora möjligheter och kritiska säkerhetsutmaningar. Då säkerhetsrisker ökar, ökar även kraven på människans kunskaper och därmed även kraven på lärande. För att minska hoten kan motiverande och upplevelsebaserat lärande, som ger utrymme för analys och reflektion, vara avgörande. Denna studie har undersökt hur man med hjälp av ett interaktivt verktyg, med användbarhet och design i centrum, kan förebygga säkerhetsrisker för företag.

Populärvetenskaplig sammanfattning av Anna Dahlström & Felicia Gabrielli Augustsson
Orginaltitel på studie: How to Educate an Organization in Working with Security Topics from a User Experience Perspective

Behovet av kvalitetssäkrade säkerhetsutbildningar växer och ställer därför användbarhet och lärande på sin spets. I takt med teknikens utbredning på arbetsplatserna har hackarnas list vuxit, vilket resulterar i en utmaning för människans säkerhetskunskaper som i många fall i ovisshet klickar på luriga länkar och laddar ner skadlig mjukvara. Det är inte bara privatpersoner som kan bli utsatta för hackarens illvilja, utan fler och fler företag faller offer för cyberattacker. Företag vidtar därför ofta proaktiva åtgärder genom att erbjuda sina anställda säkerhetsutbildningar inom cybersäkerhet och mjukvarusäkerhet. Dock anses dessa utbildningar ofta vara oengagerande, och många dundrar igenom dem snabbt som blixten istället för att ta till sig den viktiga informationen.

För att identifiera vilka krav som finns på en säkerhetsutbildning genomförde tjugo deltagare med teknisk bakgrund ett inledande test, dels bestående av självskattningsfrågor om deras kunskaper inom säkerhet, och dels bestående av kunskapsfrågor om mjukvarusäkerhet. Därefter utreddes även vilka säkerhetshot det finns mot ett it-företag. Detta gjordes genom att olika säkerhetshot utvärderade utifrån hur stor skada de kunde medföra. Kunskapstestet och hotanalysen resulterade i tre fokusområden vad gäller mjukvarusäkerhet.

Genom en kreativ process bestående av allt från brainstorming, fritt tänkande, och användartester av konceptuella idéer mynnade arbetet till slut ut i ett utbildningsbaserat

datorspel. Spelet fokuserade på de tre fokusområden som kunskapstestet och hotanalysen resulterade i. Dessutom var användbarhet och design i fokus för att skapa lust till lärande. Genom att inkludera gamifiering, vilket är en process där man tar in spelinslag i icke-spelrelaterade sammanhang för att öka motivation och inläring, och upplevelsebaserat lärande i spelet undersökte studien hur ett interaktivt verktyg kunde uppnå en högre nivå av inläring.

”Riktigt kul! Bra sätt att utbilda på.”
-Deltagare i studien

Den interaktiva lösningen jämfördes med en traditionell PowerPoint-utbildning innehållande motsvarande information genom att hälften spelade spelet och hälften genomgick den traditionella utbildningen. Direkt efter, samt två veckor efter att de genomgått utbildningen fick alla deltagare återigen genomföra ett kunskapstest. Det visade sig att de som hade läst Powerpointen presterade marginellt bättre än de som spelade spelet direkt efter utbildningen. Två veckor senare var dock resultatet omvänt, och de som spelade spelet presterade till och med bättre än två veckor tidigare, medan de andra tappade mycket av sin kunskap och nästan föll tillbaka till kunskapsnivåerna före utbildningen. Resultaten från självskattningsfrågorna visade dessutom att de som hade spelat spelet skattade sig själva högre än de som genomgick den traditionella utbildningen.