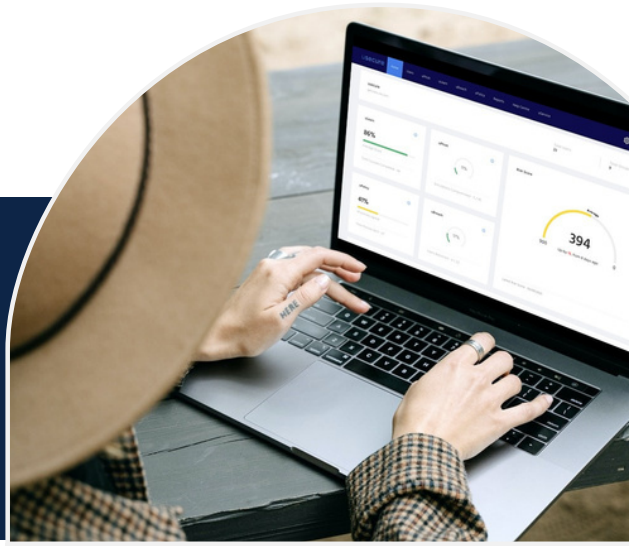
ABSEC.NO

HUMAN RISK MANAGEMENT (HRM) KASUSSTUDIE

Se hvordan HRM forvandlet denne bedriftens ansattes sikkerhetsoppførsel.



KUNDEMÅL

- Identifisere hvilke ansatte som har høy risiko for å bli kompromittert i et phiskeangrep
- Få et kontinuerlig overblikk over hvilke ansatte som er sårbare for phiskeangrep
- Levere regelmessig nettsikkerhetstrening som vil bidra til å øke brukernes motstandskraft mot phiskeangrep, samt forbedre generell sikkerhetsatferd
- Vise samsvar med ISO 27001 paragraf 7.2.2

TILNÆRMING

Nettsikkerhetstrening

- Analyser hver brukers nåværende styrker og svakheter rundt nettsikkerhet ved hjelp av en Gap Analysis Quiz.
- Ved å bruke resultatene fra quizen vil hver ansatt motta et nytt kurs for sikkerhetsbevissthet hver fjerde uke, med kurs som blir prioritert for å imøtekomme deres svakeste områder først.
- Tilpassede samsvarskurs vil også bli levert med jevne mellomrom.

Simulerte phiskeøvelser

- Minst en phiskesimulering vil bli lansert hvert halvår for å teste effekten av opplæringen og for å identifisere eventuelle høy-risikobrukere.
- Øyeblikkelig oppfølging vil bli distribuert til alle ansatte som faller for den falske e-posten under en phiske-simulering, for å redusere risikoen så snart som mulig.

Dark Web-overvåking

- Pågående dark web-overvåking vil foregå for å identifisere og unngå angrep i den tidlige fasen som utnytter stjålet ansattes legitimasjon, som for eksempel lekkede brukernavn og passord.

KUNDEPROFIL

Industri

- Bygg og anlegg

Brukertall

- 250 ansatte

Brukt plattformen siden

- August 2020

UTFORDRINGER/ HOVEDGRUNNER

- Ansatte ble kompromittert i et "gavekort"-phiskeangrep
- Nåværende opplæringsmateriell for sikkerhetsbevissthet er uengasjerende og lite effektivt
- Nåværende tilnærming til sikkerhetsbevissthet tar for lang tid

RESULTATET - RISIKOSCORE

For å måle virkningen av kundens HRM-program ble viktige risikomålinger tatt både helt i starten av programmet og etter syv måneders aktivitet.

Nedenfor kan du se risikoscoren for selskapet (alle risikomålinger satt sammen). Dette er en risikoscore på kursdeltakelse, (en kombinasjon av kurskarakterer og score), en risikoscore på phisking (de sammenlagte 'åpnet', 'klikket' og 'kompromittert'-resultatene under phiskesimuleringer) og en risikoscore på Dark Web-resultater (basert på hvor mye av virksomhetens sensitive data som har blitt lekket på det mørke nettet).

RISIKOSCORE

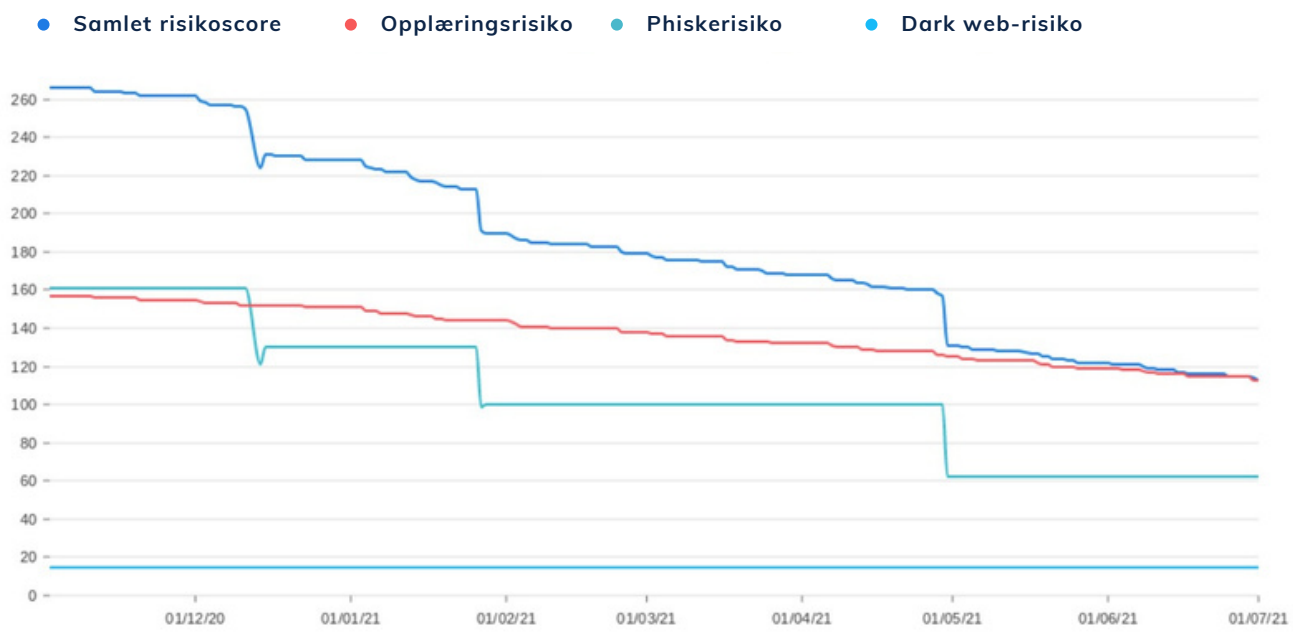
Etter å ha gjennomført syv måneder med opplæring i sikkerhetsbevissthet, periodiske simulerte phiskeøvelser og skanninger på det mørke nettet, ble kundens samlede menneskelige risikoscore redusert med 152 poeng - og flyttet dem fra medium risiko til lav risiko.

Phiske-risikoen i virksomheten falt drastisk med 100 poeng, noe som betyr at de ansatte var betydelig flinkere til å oppdage, unngå og rapportere mistenkte angrep.

RISIKOSCORE VED OPPSTART		RISIKOSCORE ETTER 7 MÅNEDER
270/900	»	**118**/900
Medium		Lav

NØKKELDATA

- FIRMARISIKO | **-152**
- OPPLÆRINGSRISIKO | **-40**
- PHISKERISIKO | **-100**
- DARK WEB-RISIKO | **INGEN ENDRING**



RESULTATET - OPPLÆRING & PHISKERESULTATER

For å redusere menneskelig cyberrisiko, var det viktig å sikre at ansatte fullførte sine kurs om sikkerhetsbevissthet så fort som mulig og nådde minimumsscoren på 80% på kursene.

For å sikre at dette skjedde, ble kursstart og kurskarakter sporet for hver ansatt, med automatiske e-postmeldinger om kurspåminnelse sendt ut til alle ansatte som ikke hadde fullført kurset i løpet av noen få arbeidsdager.

De pågående phiske-simuleringsresultatene ble også sporet for å sikre at opplæringskursene for sikkerhetsbevissthet hadde ønsket innvirkning.

OPPLÆRING

Gjennomsnittlig tid å fullføre et kurs etter påmelding	Kurs startet	Kurs tatt	Gjennomsnittlig kursscore
3 dager	97%	97%	92%

PHISKESIMULERINGSRESULTATER

	Sendt	Åpnet	Besøkt	Kompromittert
Første simulering	146	74	40	9
Andre simulering	172	34 -74%	4 -163%	2 -127%

Av de 250 ansatte, fullførte 97% prosent kursene sine, og tok i gjennomsnitt bare tre dager å fullføre kurset etter påmelding, mens de i gjennomsnitt scoret 92%.

Som det beviser i phiskesimuleringstabellen over, var det mye mindre sannsynlig at ansatte åpnet, klikket eller ble kompromittert av en phiskesimulering etter kursdeltakelsen.