GÖRAN TOMTE

ZERO TRUST

SOLDIER

https://gorantomte.no/

https://zerotrustsoldier.com/

Hvorfor er dere her i dag?

«Det er jo så fint, så det må jo være bra»

Hvor går grensa mellom sky og tåke?

Når det fine kommer med nye sårbarheter

Phishing

Sosial manipulasjon

Start til Slutt
eller
Slutt til Start

Dagens trusselbilde

er så mangt

Løsepengeangrep
Svindel
Sabotasje
Spionasje

GØRAN TØMTE

MFA fungerer

derfor er det ikke lenger godt nok

November 4, 2023

NRK ble svindlet for en million. Slik kunne det vært avverget.

NRK ble nettopp svindlet for 80.000,- Euro. Teknikkene de kriminelle benyttet er relativt ferske. Det er meget viktig at alle får med seg detaljene om hvordan dette angrepet var mulig, og enda viktigere at alle forstår hvordan alle kan beskytte seg mot slike angrep.

NRK sa etter angrepet:

Dette har vært et så avansert angrep at det er krevende å oppdage, og det er samfunnsmessig veldig alvorlig, sier teknologidirektør Pål Nedregotten i NRK.

Men er det egentlig så krevende?

https://zerotrustsoldier.com/2023/11/04/nrk-ble-svindlet-for-en-million-slik-kunne-det-vaert-avverget/

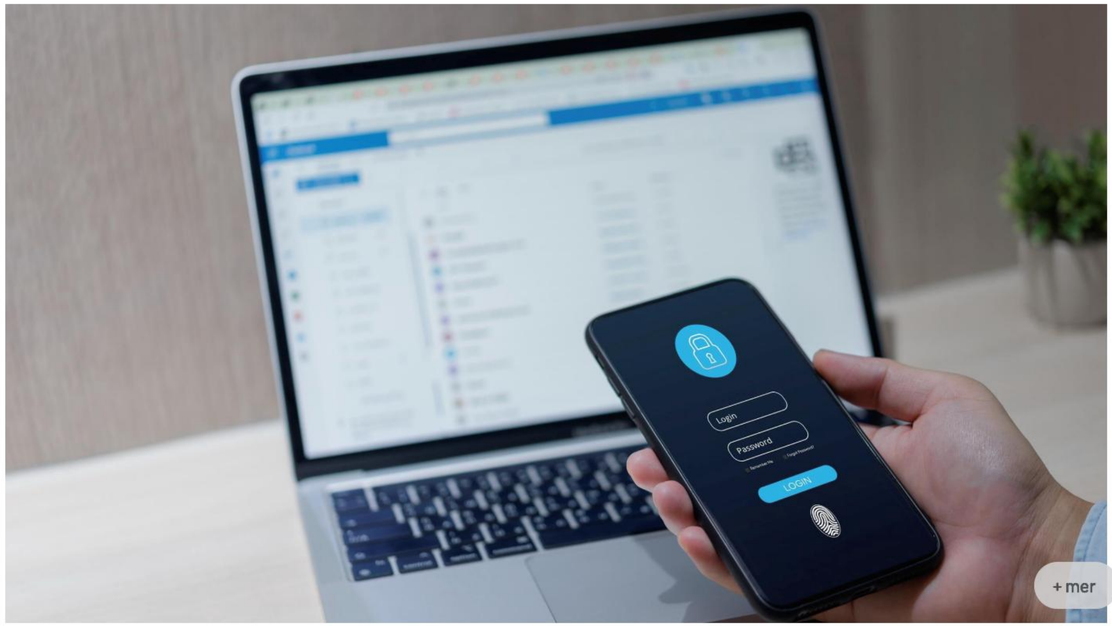
GÖRAN TÖMTE

Hundrevis utsatt for datainnbrudd – hvorfor reagerer ingen?

I det digitale domenet går datainnbruddene og tyveriene under radaren. Det må vi endre på, skriver Simen Bakke.

Publisert 2. feb.

Lesetid: 3 minutter



IKKE LENGER SIKKERT: Årsaken til den enorme økningen er at de cyberkriminelle nå kommer seg forbi tofaktorautentiseringen, skriver a... Mer

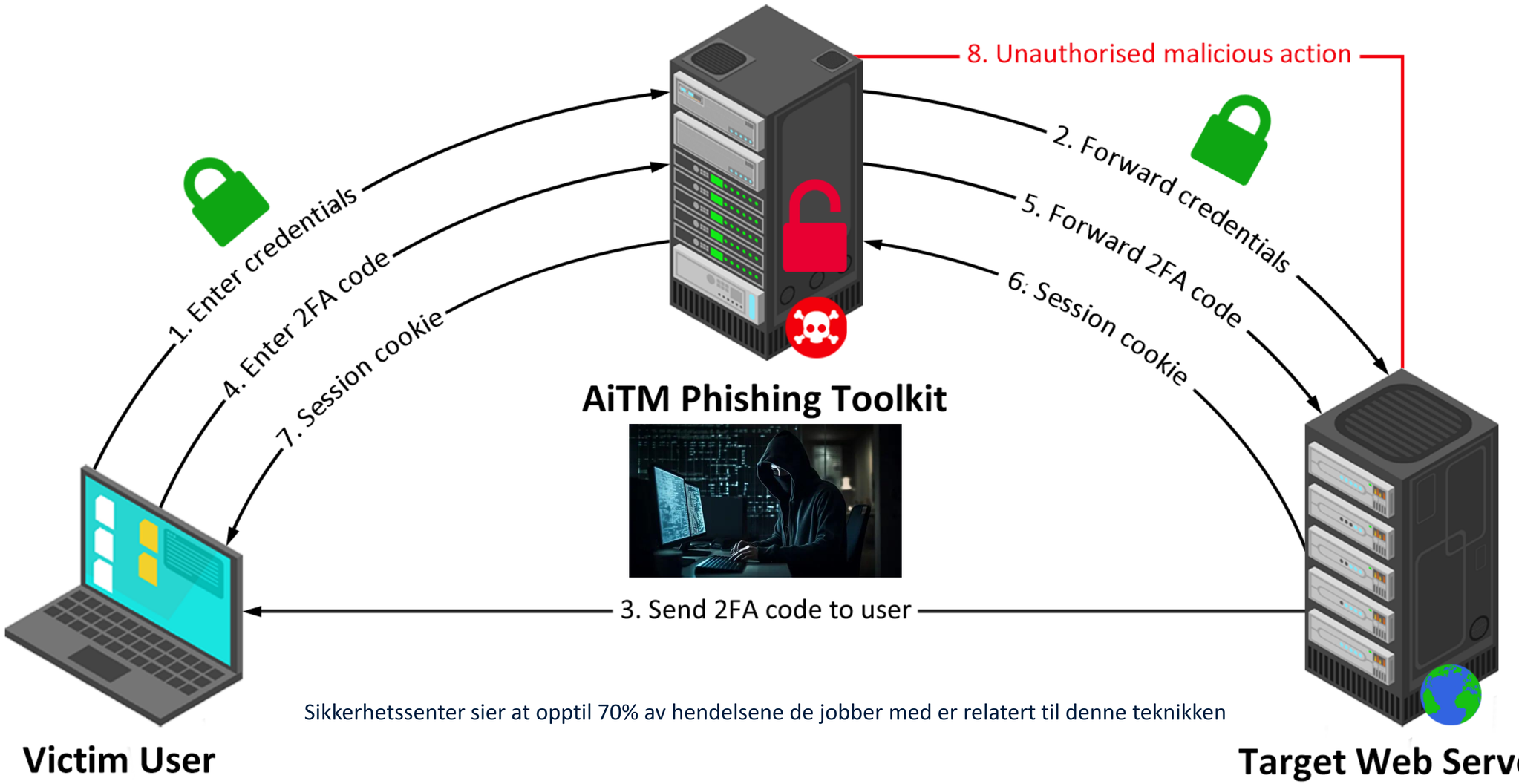
Teknologi

Simen Bakke
Senior informasjonssikkerhetsrådgiver i Politiets IKT-tjenester

https://www.finansavisen.no/teknologi/2025/02/02/8236925/hundrevis-utsatt-for-datainnbrudd-hvorfor-reagerer-ingen

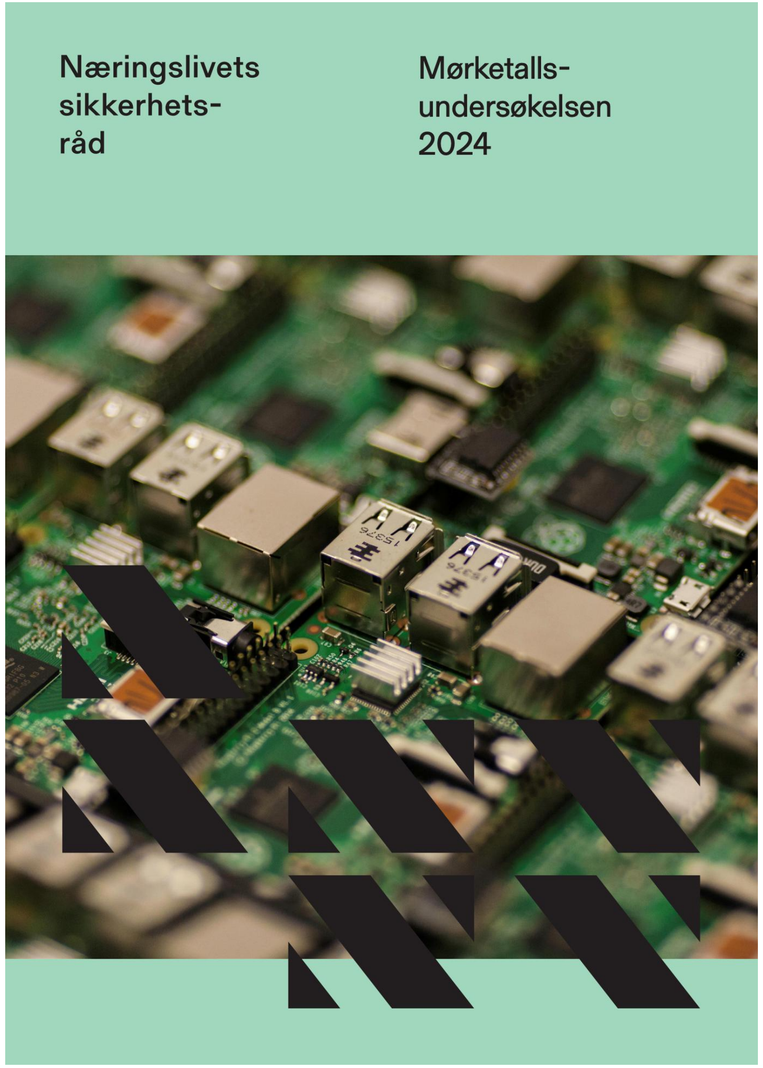
GÖRAN TÖMTE

Hva er AiTM, Adversary in The Middle, og hvordan fungerer det?



Sikkerhetssenter sier at opptil 70% av hendelsene de jobber med er relatert til denne teknikken

https://www.pentestpartners.com/security-blog/intercepting-mfa-phishing-and-attackers-in-the-middle/



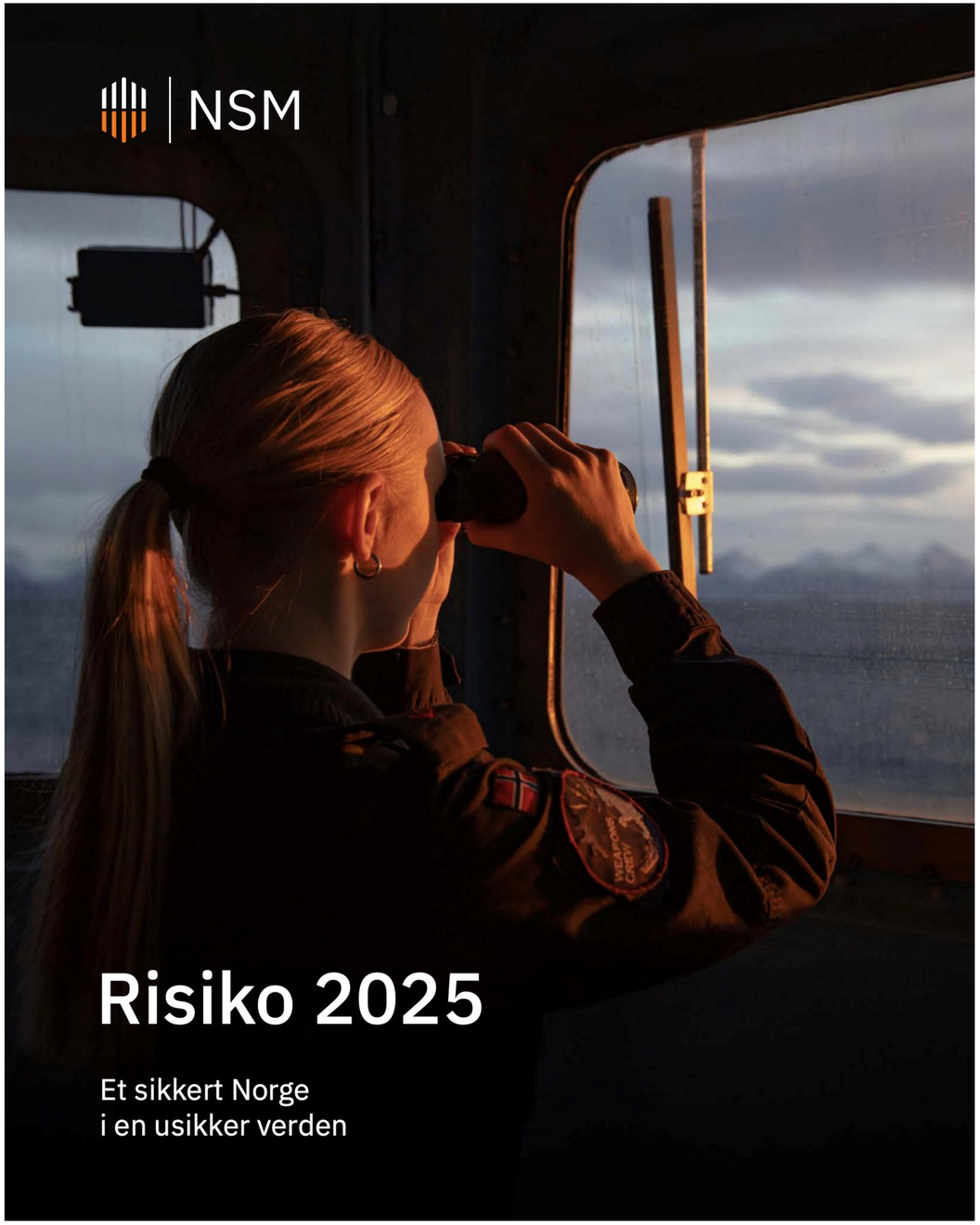
1. Identifisere og kartlegge

For å håndtere risikoen knyttet til eksponerte tjenester, bør virksomheter først gjennomføre regelmessige risikovurderinger og kartlegge hvilke systemer og applikasjoner som er tilgjengelige på Internett. Mange virksomheter er ikke klar over hva de eksponerer, noe som gjør dem sårbare for angrep.

I tillegg er det viktig å implementere sikkerhetsoppdateringer og patching uten forsinkelse, samt bruke sterke autentiseringsmekanismer som flerfaktorautentisering (MFA) for å beskytte eksponerte tjenester. I denne sammenheng bør sikkerhetsstyrken til de ulike MFA-løsningene vurderes, og her fremhever vi spesielt phishing-resistent MFA som FIDO og PKI-baserte løsninger. Nettverkssegmentering og isolering av kritiske systemer kan også bidra til å begrense konsekvensene av et angrep.

2. Beskytte og opprettholde

For å sikre hybride infrastrukturer er det avgjørende å etablere en robust arkitektur og riktig konfigurasjon og herding av skytjenester. Det er spesielt viktig i denne sammenheng å ha full kontroll over API-nøkler og aksesstoken, og sørge for at omfanget (scope) for disse nøklene er redusert til et absolutt minimum innenfor de tjenesteområdene de brukes til.
I hybride arkitekturer er det essensielt å ha kontroll på identitets- og tilgangsstyring. Effektiv beskyttelse og kontroll av tilganger er avgjørende for å hindre misbruk, spesielt med et økt fokus på «credential harvesting»-operasjoner fra kriminelle aktører. En nyere endring er at økt bruk av MFA har ført til utviklingen av angrep som forsøker å omgå slike mekanismer, som for eksempel Adversary in The Middle («AiTM»). Virksomheter bør tilstrebe å etterleve «least privilege»-prinsippet for sine identiteter, og kartlegge mulige bevegelseskanaler fra sky- til on-premise miljøer.



Løsepengeangrep anses som den største utfordringen for norske virksomheter, ifølge en gjennomgang fra de sektorvise responsmiljøene i Norge. Responsmiljøene skal forebygge og håndtere digitale kriser i egen sektor. Løsepengeangrep er en type angrep hvor en aktør bryter seg inn i en virksomhets IKT-systemer for å kryptere og stjele virksomhetens data. Deretter prøver angriperen å presse målet for penger i bytte mot en nøkkel eller et verktøy for å dekryptere dataene samt å ikke lekke eller selge de stjålne dataene. Selv om kriminelle aktører selv får større utbytte fra andre typer svindel, påfører løsepengeangrep større skade for berørte virksomheter på grunn av stopp i drift.

Angrepsmetoden rettes ofte mot små og mellomstore virksomheter. Selv om virksomhetene ikke forvalter samfunnsviktige funksjoner kan angrepene likevel få større konsekvenser hvis selskapene har informasjon om kundeforhold, leveranser eller leverandørkjeder som kan være attraktiv å selge. Informasjon knyttet til nasjonale verdier kan på denne måten bli kjøpt av utenlandske etterretningstjenester.

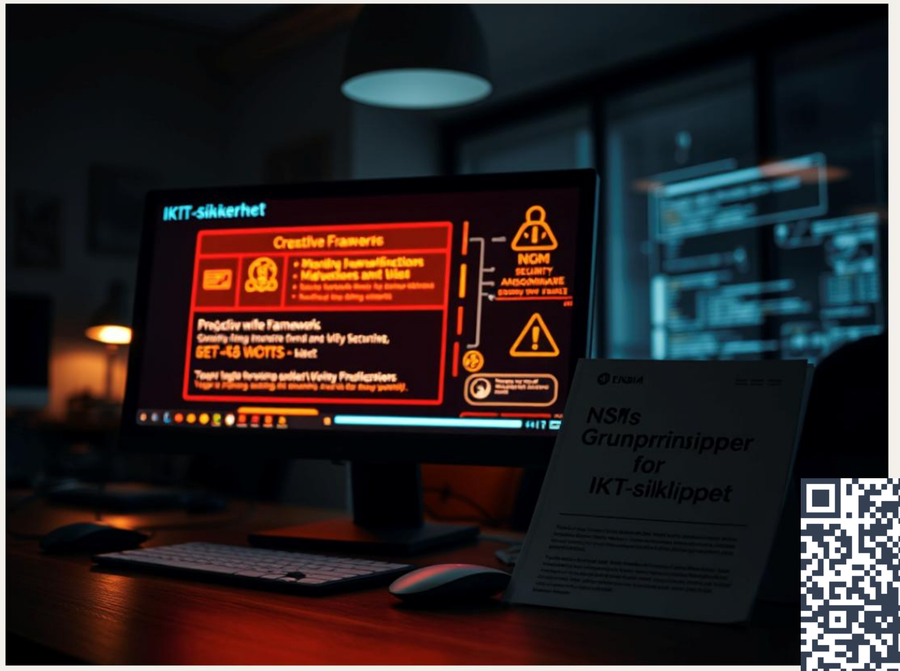
Angriper-i-midten (eng: adversary-in-the-middle) er en type phishingangrep som det seneste året har rammet et betydelig antall norske virksomheter. Ved å operere mellom offeret og en påloggingsnettside kan angriperen lure til seg passord og komme seg forbi flerfaktorautentisering. E-postkontoer er attraktive mål fordi de gjennom målrettet sosial manipulasjon kan brukes til svindel eller for å komme seg inn i virksomhetens nettverk og systemer. Trusselaktører kan også utnytte tilgangen for å få innsyn i og manipulere kommunikasjon internt i virksomheten eller med eksterne partnere. I tillegg kan angriperen potensielt også få tilgang til skybaserte tjenester, som Microsoft 365 eller Google Workspace. Angriperen får da tilgang og mulighet til å hente ut filer som er lagret i tjenesten.

GÖRAN TÖMTE

Konklusjon

March 25, 2025

Vent med NSMs Grunnprinsipper for IKT-sikkerhet

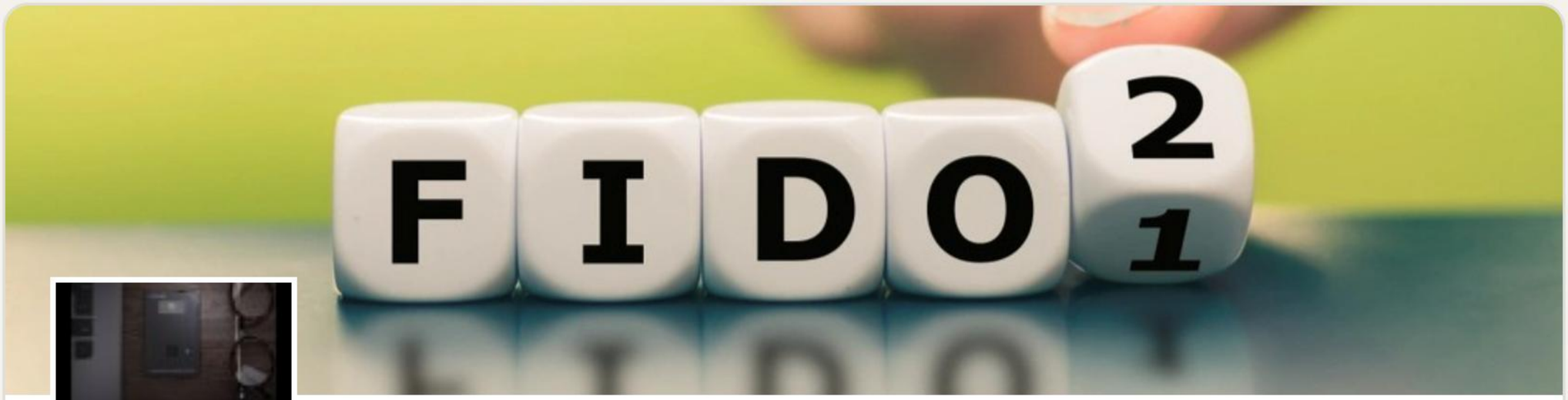


Sikkerhet er komplisert, men å sikre seg kan være meget enkelt.

Rammeverk, på godt og vondt, om det er NSMs Grunnprinsipper for IKT-sikkerhet, ISO 27001, NIST CSF, CIS CSC, eller annet…. De er store, omfattende, tidkrevende og til dels kompliserte.

https://zerotrustsoldier.com/2025/03/25/vent-med-nsms-grunnprinsipper-for-ikt-sikkerhet/

GÖRAN TÖMTE



Phishingresistant FIDO2 erfaringsutveksling

Public group

Earn an Active Group badge

https://www.linkedin.com/groups/10020701/

NSM

NSM anbefaler overgang til phishingresistent autentisering

Publisert: 12.12.2024 Oppdatert: 17.12.2024

NSM anbefaler virksomheter å gå over til passnøkler (passkeys) eller andre FIDO2-implementasjoner for autentisering. Årsaken er at aktører i økende grad tar seg forbi tradisjonell flerfaktorautentisering.

NSM har registrert en rekke phishingkampanjer der målet er økonomisk vinning, ofte via fakturasvindel. Kampanjene lar seg gjennomføre fordi virksomheter ikke påkrever phishingresistent autentisering.

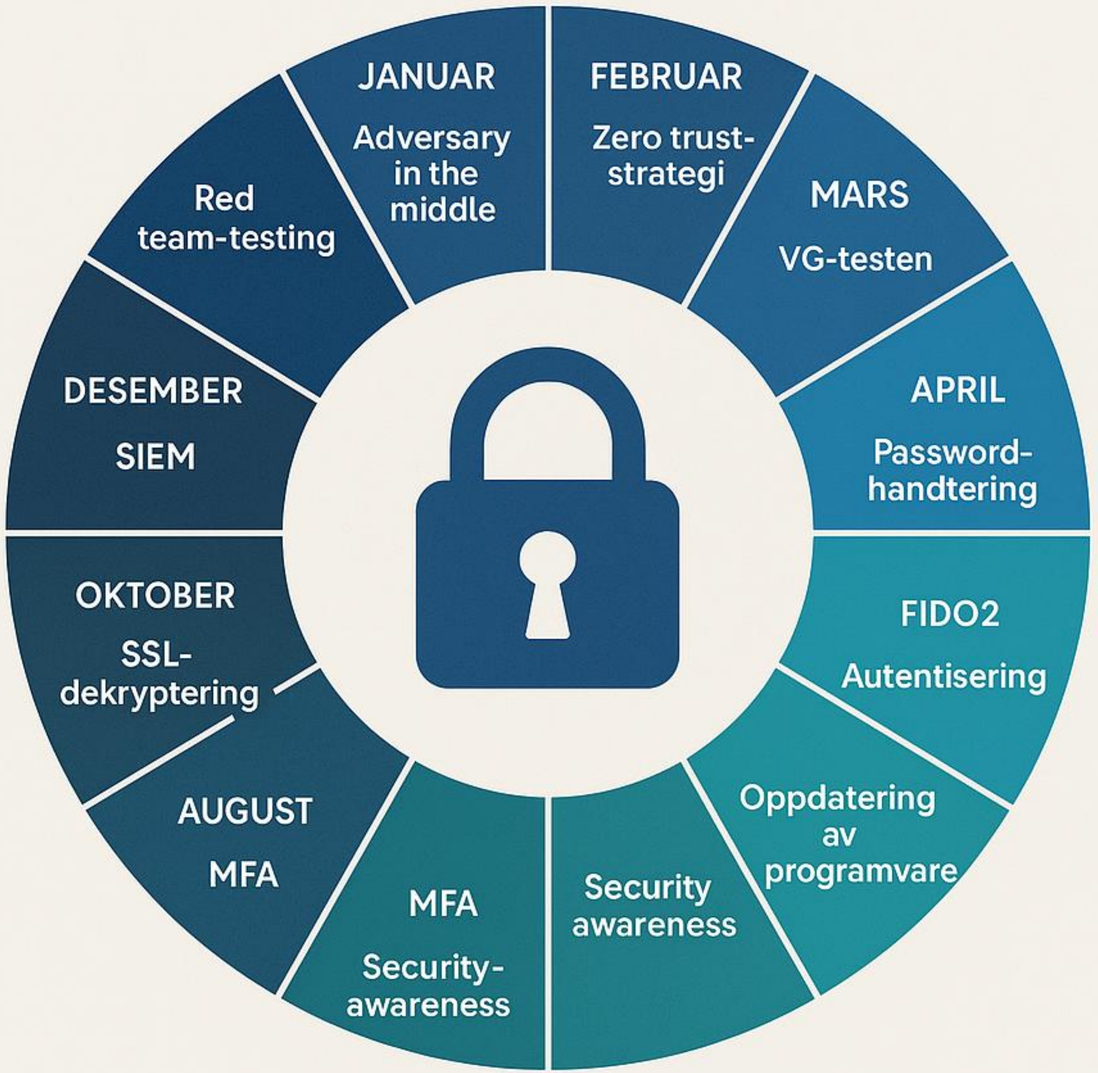
Passnøkler erstatter passord og tradisjonelle flerfaktorløsninger. Passnøkler er teknologien industrien har standardisert seg på, og støttes av populære nettlesere, operativsystemer, mobiltelefoner, identitetsløsninger og skyløsninger.

Passnøkler hindrer angrepsmetoder der en angriper har tilgang til eller prøver å få tilgang til brukers passord. Dette inkluderer phishing, varselutmattelse, angriper-i-midten (AitM) og bruteforce. Passnøkler fjerner også risikoen med svake og gjenbrukte passord. Passnøkler oppnår dette ved å overta autentiseringsansvaret fra brukeren, slik at trusselaktører verken kan stjele eller lure til seg passnøklene.

https://nsm.no/fagomrader/digital-sikkerhet/nasjonalt-cybersikkerhetssenter/varsler-fra-ncsc/nsm-anbefaler-overgang-til-phishingresistent-autentisering

GÖRAN TÖMTE

ÅRSHJUL FOR CYBERSIKKERHETSTTILTAK



Entra ID optimalisering (gratis)
Windows Hello for Business (gratis)
FIDO2

Brukervennlighet OG sikkerhet på en og samme gang
Det har vel aldri skjedd før?

GÖRAN TÖMTE

TAKK FOR MEG

Blogg

Webside

LinkedIn

GÖRAN TÖMTE