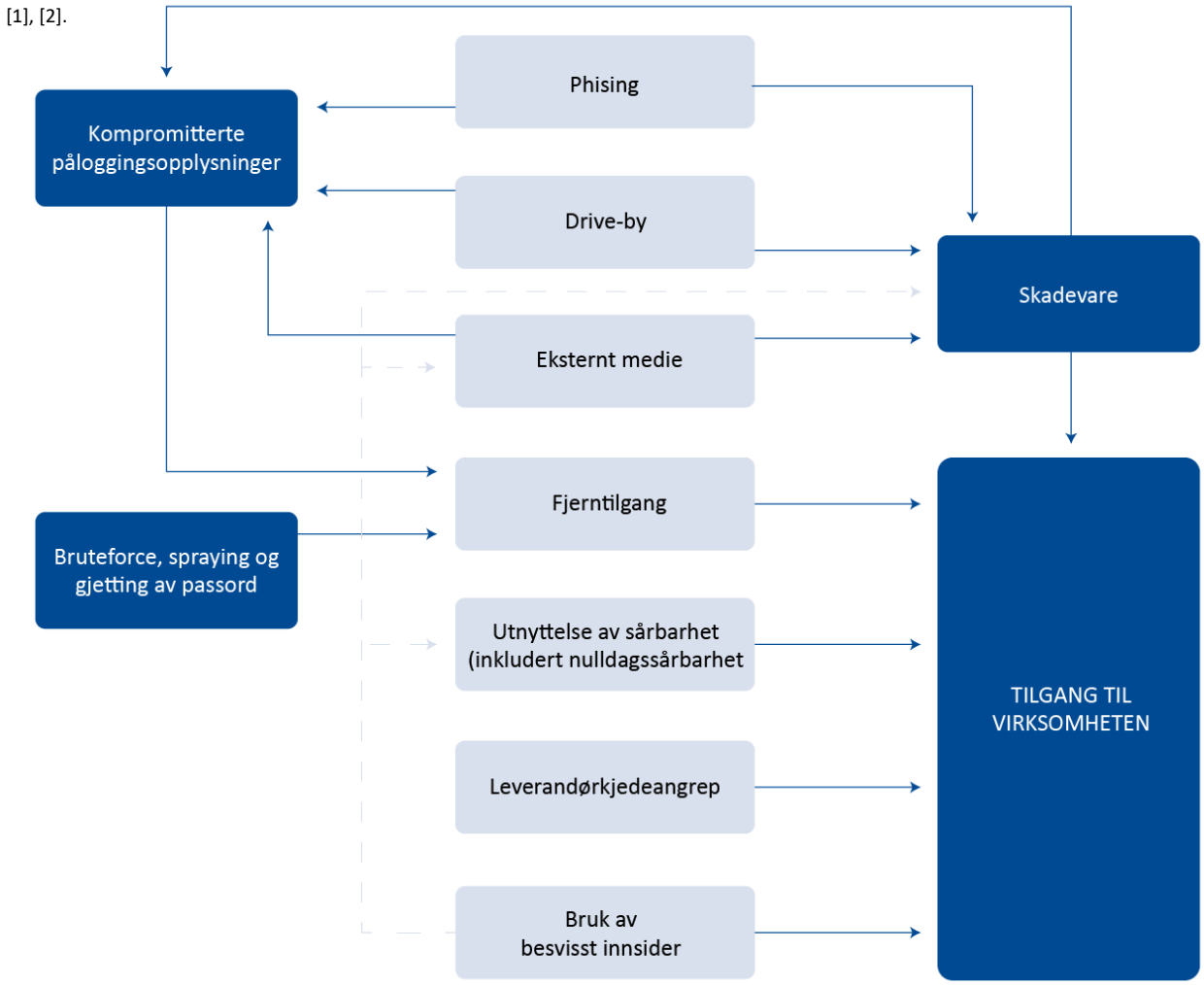
ANGREPSVEKTORER FOR INITIELL TILGANG

[1], [2].



Phishing

Phishing er en form for sosial manipulering via e-post som lurer en person på innsiden av virksomheten til å gi fra seg påloggingsopplysninger eller laste ned skadevare på virksomhetens system [3]. Dette gjøres ofte ved å lure den ansatte i en virksomhet til å klikke på lenker i tilsynelatende troverdige e-poster [4], [5]. Trusselaktørene bak phishing har de senere årene brukt bedre språk [6], dette blir nå ytterligere forsterket av at aktørene kan benytte kunstig intelligens. Språkbarrieren viskes gradvis ut og dette kan øke sannsynligheten for at trusselaktøren lykkes.

Spear phishing er en målrettet form for phishing, her har gjerne aktøren utført rekognosering i forkant for å skreddersy e-posten til å lure enkeltpersoner [5].

Utnyttelse av sårbarheter i internetteksponerte tjenester og servere

Trusselaktører kan utnytte sårbarheter i internetteksponerte tjenester og servere. Det vanligste her er å utnytte kjente sårbarheter som offeret ikke har rukket å sikkerhetsoppdatere, eksempler her er ProxyLogon, ProxyShell og Log4Shell [7].

En nulldagssårbarhet er en sårbarhet i en programvare som ikke er kjent for leverandøren før den utnyttes av trusselaktører, en ukjent sårbarhet. Så snart en nulldagssårbarhet blir kjent av leverandøren og offentligheten, vil det ikke lenger være en nulldagssårbarhet.

Utnyttelse av fjerntilgang
Utnyttelse av fjerntilgangsløsninger kan for eksempel være å skaffe initiell tilgang til et system via Remote Deskop Protocol (RDP) eller Virtual Private Network (VPN). For å få tilgang er det vanlig å utnytte sårbarheter som manglende flerfaktorautentisering i kombinasjon med svake eller gjenbrukte passord [8].

Påloggingsopplysninger (passord)
Som man ser av modellen spiller «kompromitterte påloggingsopplysninger» og «bruteforce, spraying og gjetting av passord» en sentral rolle i mange ulike angrepsvektorer. Metodene defineres ikke i denne rapporten som angrepsvektorer i seg selv, men er likevel en viktig faktor i mange angrep. Spesielt i fasen for initell kompromittering men også i de videre fasene i cyber attack lifecycle. Fellesnevneren her er at trusselaktøren benytter seg av passord for å komme videre i angrepet. Dette kan gjøres på flere ulike måter.

Brute-forcing: Bruk av datakraft for å teste svært mange passord på kort tid, ofte i form av en strukturert tilnærming ved for eksempel å teste de tusen mest brukte passordene først. Beskyttelse mot dette kan blant annet være at kontoen låses etter fem mislykkede påloggingsforsøk.

Spraying: Sistnevnte sikkerhetsmekanisme kan omgås dersom man har et stort antall brukere og deres brukernavn tilgjengelig. Da kan man velge ut fem av de vanligste passordene og bruke datakraft til å teste passordene på alle brukerkontoene samtidig. Dette kalles spraying.
Gjette passord: Passordet kan simpelthen være så svakt at det er lett å gjette. En aktør kan også gjette vanskeligere passord ved bruk av sosial manipulering eller sammenstilling av informasjon om brukeren ved bruk av åpne kilder.

Stjålne påloggingsopplysninger: Brukernavn og passord på avveie kan også brukes. Det kan være store mengder brukernavn og passord som er hentet ut i et annet angrep og ligger tilgjengelig på internett. Her kan en trusselaktør for eksempel utnytte at en person bruker samme passordet på flere tjenester. Som vi ser av modellen kan dette også være brukernavn og passord som er kompromittert tidligere i angrepet med bruk av andre metoder som for eksempel phishing eller skadevare.

Drive-By kompromittering
I dette tilfellet kompromitterer trusselaktøren en nettside, besøkende til denne nettsiden blir deretter forsøkt kompromittert gjennom ukjente og/eller ikke oppdaterte svakheter i nettleser. Gjøres dette mot en nettside angriper forventer at besøkes hyppig av interessante mål kalles det gjerne for et «vannhullsangrep» [2].

Bruk av eksternt medie
En trusselaktør kan også skaffe seg tilgang ved bruk av eksternt medie, eksempelvis en USB-minnepinne. Det eksterne mediet fungerer som bærer for skadevare som kjøres enten av angriper selv, eller uforvarende av en bruker gjennom sosial manipulering [2].

Leverandørkjedeangrep
Leverandørkjedeangrep innebærer at trusselaktører for eksempel utnytter programvare- og tjenesteleverandører for å få klarert tilgang i systemene til leverandørens kunder. Skytjenester (Managed Service Providers), IT leverandører og Enterprise Managed Software Systems er attraktive mål i forbindelse med slike angrep [9], [10], [11]. Leverandørkjedeangrep er en spesielt effektiv metode fordi den misbruker den iboende tilliten virksomheter har til IKT utstyr, programvarer og oppdateringer som mottas fra pålitelige leverandører. På den måten omgår denne typen angrep mange av sikkerhetsmekanismene som brukes for å forebygge og oppdage angrep. I tillegg ser flere aktører på kompromittering av leverandørkjeder som en effektiv metode fordi en enkelt kompromittering potensielt kan gi tilgang til et stort antall andre virksomheter [12]. NSM viser til at flere virksomheter det siste året har fått et mer bevisst forhold til denne problematikken, men påpeker at leverandørkjedeangrep fortjener oppmerksomhet fordi dette utnyttes aktivt av trusselaktørene [13], [14].

Bruk av innsidere
En innsider kan gjøre følgende skade:
- Stjele informasjon
- Lekke eller offentliggjøre informasjon
- Slette informasjon, som for eksempel e-poster som beviser kommunikasjon i en prosess
- Sabotere tilgjengeligheten eller integriteten til et system
- Påvirke eller manipulere personer
- Hjelpe å tilrettelegge for andre aktører i form av avlytting, bistand i dataangrep, informasjon om sårbarheter og sikkerhetstiltak.

[15].

De tre første kategoriene av innsidere, definert nedenfor, har alle til felles at de benyttes som et verktøy eller metode av en trusselaktør. Dette er ikke tilfellet for den siste kategorien, hvor innsideren selv har en motivasjon for å utøve

innsidevirksomhet.

Den **ikke-selvmotiverte bevisste innsideren** er en person som blir rekruttert av en trusselaktør etter at personen har fått tilgang til virksomhetens verdier og systemer. En slik person har ikke nødvendigvis en intensjon om å bli en innsider, men kan for eksempel være mottakelig for bestikkelser, ha en lojalitet som kan være mulig å påvirke eller ha sårbarheter som gjør vedkommende mulig å presse [15].

Den **ikke-selvmotiverte ubevisste innsideren** kan oppstå ved at en trusselaktør forleder, manipulerer eller på annen måte utnytter en person for å få tilgang til en virksomhets verdier og systemer. I slike tilfeller vil den aktuelle personen være en kapasitet for trusselaktøren, uten at personen selv er bevisst dette. Handlinger som begås av ubevisste innsidere kan ofte knyttes til lav sikkerhetsforståelse [15].

Infiltratøren er en person som bevisst søker seg legitim tilgang til en virksomhet og dens verdier med den intensjon om å begå innsidevirksomhet, det vil si at intensjonen er der før et eventuelt ansettelsesforhold. Infiltratøren kan være direkte underlagt en trusselaktør eller være rekruttert [15].

En selvmotivert bevisst innsider er ikke motivert av en trusselaktør, men har en egen motivasjon for å utøve innsidevirksomhet som kan få skadefølger for virksomheten [15].

Kilder

[1] Center for Cybersikkerhed, cfcs, «Trusselvurdering: Fjern adgangen,» Center for Cybersikkerhed, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/trusselsvurdering-fjern-adgangen.pdf, 2021.

[2] ATT&CK, MITRE, «attack.mitre.org,» ATT&CK Matrix for Enterprise, 2023. [Internett]. Available: https://attack.mitre.org/.

[3] Nasjonal Sikkerhetsmyndighet, «Risiko 2022,» 2022.

[4] Politiets Sikkerhetstjeneste, «Nasjonal trusselvurdering,» 2023.

[5] Politiet, «Politiets trusselvurdering 2022,» 2022.

[6] Nasjonal Sikkerhetsmyndighet, «Digitalt risikobilde 2021,» 2021.

[7] European Union Agency for Cybersecurity, «ENISA Threat Landscape,» 2022.

[8] Mandiant, «M-Trends 2022,» Mandiant, 2022.

[9] Health-ISAC, «Current and Emerging Healthcare Cyber Threat Landscape - Executive Summary,» 2022.

[10] European Union Agency for Cybersecurity, «ENISA Threat Landscape 2021,» 2021.

[11] Europol, «IOCTA - Internet organised crime threat assessment,» 2021.

[12] Health- Information Security and Analysis Center, «CURRENT AND EMERGING HEALTHCARE CYBER THREAT LANDSCAPE,» 2022.

[13] Nasjonal Sikkerhetsmyndighet, «Risiko 2023,» NSM, 2023.

[14] Nasjonal Sikkerhetsmyndighet, «Digitalt Risikobilde 2022,» NSM, 2022.

[15] Nasjonal Sikkerhetsmyndighet, «Temarapport Innsiderisiko,» 2018.