MITSUBISHI ELECTRIC CORPORATION
PUBLIC RELATIONS DIVISION
7-3, Marunouchi 2-chome, Chiyoda-ku, Tokyo, 100-8310 Japan

FOR UMIDDELBAR UTGIVELSE **nr. 3649**

Denne teksten er en oversettelse av den offisielle engelske versjonen av pressemeldingen, og den er kun ment som et referanseverktøy. Du finner detaljene og spesifikasjonene i den originale engelske versjonen. Dersom tekstene ikke stemmer overens, er det den originale engelske versjonen som gjelder.

Kundeforespørsler

Information Technology R&D Center
Mitsubishi Electric Corporation

www.MitsubishiElectric.com/ssl/contact/company/rd/form.html

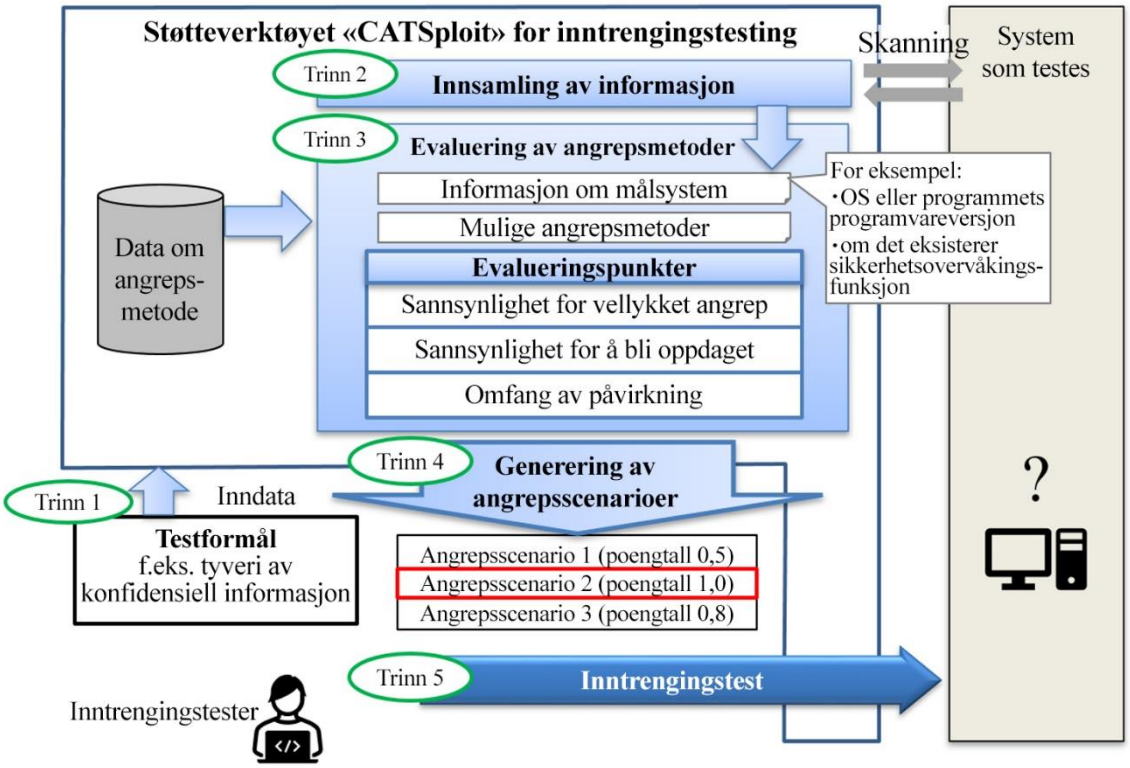
Medieforespørsler

Public Relations Division
Mitsubishi Electric Corporation

prd.gnews@nk.MitsubishiElectric.co.jp
www.MitsubishiElectric.com/news/

Mitsubishi Electric utvikler verdens første støtteverktøy for inntrengingstest som genererer angrepsscenarioer fra hackerperspektiver

Forventes å forbedre motstandsdyktigheten mot cyberangrep for alle produkter som er koblet til nettverk



Eksempel på bruk av støtteverktøyet under inntrengingstesting

TOKYO, 5. desember 2023 – Mitsubishi Electric Corporation (TOKYO: 6503) kunngjorde i dag at de har utviklet verdens første[1] støtteverktøy for inntrengingstest[2], CATSploit, som automatisk genererer angrepsscenarioer basert på testmålene til en inntrengingstester, som for eksempel tyveri av konfidensiell informasjon, for å evaluere hvor virkningsfulle testangrep er. Selv uerfarne sikkerhetsteknikere kan enkelt utføre inntrengingstester ved hjelp av angrepsscenarioene og de påfølgende testresultatene (poengene).

I løpet av de siste årene har kontrollsystemer, inkludert infrastruktur, fabrikkutstyr osv., blitt stadig mer koblet til nettverk, noe som øker risikoen for avbrudd, for eksempel strømbrudd eller driftsstans for offentlig transport, på grunn av cyberangrep. Behovet for å iverksette sikkerhetstiltak i slike systemer har blitt presserende. I tillegg krever ISA/IEC 62443[3]-standardene at det utføres fuzzing[4]- og inntrengingssikkerhetstester på systemer og utstyr for å evaluere motstanden mot cyberangrep, inkludert sårbarheter som skyldes implementerings- eller konfigurasjonsfeil. Inntrengingstesting er svært sofistikert og krever at white-hat-hackere[5] engasjeres til faktiske angrep på systemet eller produktet som testes, men slike personer, som må ha svært høy ekspertise, er det få av, og de er vanskelige å finne.

Mitsubishi Electric har nå, ved å fokusere på faktorene som white-hat-hackere vurderer når de velger angrepsvektorene sine, utviklet et støtteverktøy for inntrengingstest som genererer lister over mulige angrepsscenarioer og hvor virkningsfulle de er (uttrykt som numeriske poeng).

Detaljer om verktøyet presenteres 6. desember (kl. 11 lokal tid) under Black Hat Europe 2023 Arsenal i London, som finner sted 6. og 7. desember.

Funksjoner

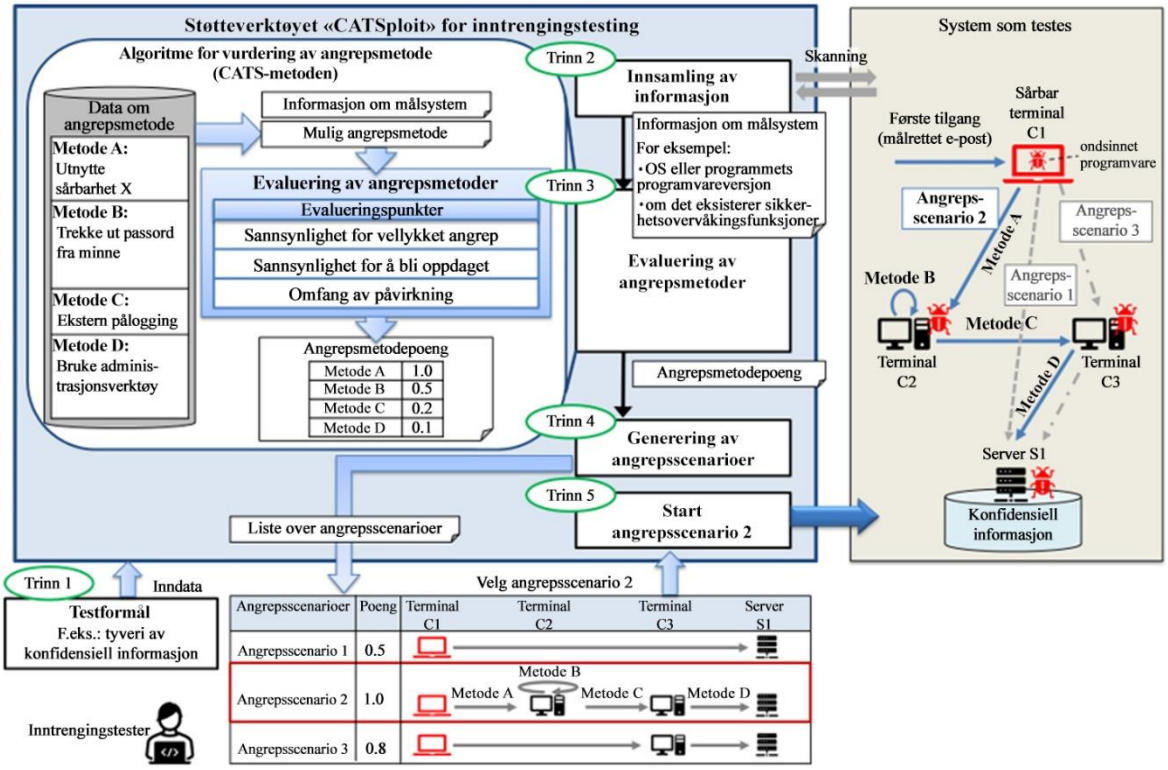
1) ***Automatisk generering av angrepsscenarioer fra en white-hat-hackers perspektiv***
   - Mitsubishi Electric fokuserte på faktorer som white-hat-hackere vurderer når de velger angrepsmetodene sine, for eksempel sannsynligheten for vellykket angrep, sannsynlighet for å bli oppdaget og omfanget av påvirkningen. Ved å justere i henhold til formålene med spesifikke tester kan systemet automatisk generere scenarioer som viser de nødvendige trinnene for å implementere et angrep for å oppnå disse formålene.

2) ***Optimale tester evaluerer angrepsscenarioers virkning fra en white-hat-hackers perspektiv***
   - Mitsubishi Electrics merkevarebeskyttede metode CATS[6] beregner hvor virkningsfull hver angrepsmetode er (uttrykt som et numerisk poeng) ut fra perspektivet til en white-hat-hacker. På grunnlag av dette foreslås det en liste over angrepsscenarioer slik at det mest virkningsfulle scenarioet (høyeste poeng) kan velges.
   - CATS-evalueringen tar ikke bare hensyn til kjent systeminformasjon, som operativsystem, programversjon og enheter for sikkerhetsovervåking, men også manglende systeminformasjon, som bidrar til å realisere angrepsscenarioer som gjengir en faktisk angripers synspunkt.

---

[1] I henhold til Mitsubishi Electrics forskning, oppdatert 5. desember 2023
[2] Test for å bekrefte om et system eller utstyr kan bli utsatt for et faktisk angrep
[3] Sikkerhetsstandarder for industristyringssystemer
[4] En testmetode for å oppdage programvarefeil eller sårbarheter ved å skrive inn ugyldige eller uriktige data
[5] Etiske hackere som bruker avansert kunnskap og datateknologi til å identifisere sikkerhetsproblemer osv.
[6] Cyber Attack Techniques Scoring: Mitsubishi Electrics merkevarebeskyttede metode for evaluering av angrepsvektorers virkning

- Den automatiske evalueringen av angrepsscenarioer som sannsynligvis vil bli brukt av white-hat-hackere, gjør at mindre erfarne sikkerhetsteknikere enkelt kan utføre inntrengingstester.



Støtteverktøyet CATSploit for inntrengingstesting

Fremtidig utvikling

For å forbedre motstandsdyktigheten mot cyberangrep for systemer og enheter utviklet av Mitsubishi Electric, vil selskapet fortsette å forske på og utvikle dette nye verktøyet med mål å bruke det til faktisk sikkerhetstesting av selskapets produkter innen 2026.

###

Om Mitsubishi Electric Corporation

Med over 100 års erfaring med å levere pålitelige produkter av høy kvalitet er Mitsubishi Electric Corporation (TOKYO: 6503) en anerkjent verdensleder innen produksjon, markedsføring og salg av elektrisk og elektronisk utstyr som brukes innen informasjonsbehandling og kommunikasjon, romfart og satellittkommunikasjon, forbrukerelektronikk, industriteknologi, energi, transport og anleggsutstyr. Mitsubishi Electric beriker samfunnet med teknologi i tråd med «Changes for the Better» (Endringer til det bedre). Selskapet registrerte en inntekt på 5003,6 milliarder yen (37,3 milliarder amerikanske dollar*) i regnskapsåret som endte 31. mars 2023. Hvis du vil ha mer informasjon, kan du gå til www.MitsubishiElectric.com

*Beløp i USD er konvertert fra yen ved kursen ¥134 = USD 1, den omtrentlige kursen på Tokyo Foreign Exchange Market den 31. mars 2023