Trusselsvurdering

Ransomware-truslen mod produktions-virksomheder

Indhold

CENTER FOR CYBERSIKKERHED

Kastellet 30
2100 København Ø
Telefon: + 45 3332 5580
E-mail: cfcs@cfcs.dk

1. udgave december 2023

Ransomware-truslen mod produktionsvirksomheder

Formålet med vurderingen er at oplyse produktionsvirksomheder om det meget høje trusselsniveau fra cyberkriminalitet. Vurderingen henvender sig til beslutningstagere i produktionsvirksomheder og kan indgå i virksomhedernes arbejde med risikoanalyser.

Produktionsvirksomheder er i trusselsvurderingen betegnet som virksomheder, der fremstiller fysiske produkter som bl.a. maskiner og medicin.

Hovedvurdering

- Truslen fra cyberkriminalitet mod danske produktionsvirksomheder er **MEGET HØJ.** Produktionsvirksomheder med samfundskritiske funktioner bliver også angrebet af ransomware-aktører, da aktørerne ikke diskriminerer i deres valg af ofre.

- Produktionsvirksomheder bliver hovedsageligt ramt af målrettede ransomware-angreb, fordi ransomware-aktørerne forventer, at virksomhederne både kan og vil betale en høj løsesum for at få dekrypteret deres data og systemer.

- Ransomware-angreb kan lede til driftsforstyrrelser samt produktionsstop og dermed økonomiske tab for virksomheden.

- Da data ofte deles mellem mange sammenkoblede systemer i produktionsmiljøer, kan et angreb på virksomhedens IT påvirke de operationelle processer. Manglende segmentering kan samtidigt give hackerne bedre mulighed for at gennemføre et skadeligt angreb. Frygten for dette kan lede til et selvvalgt produktionsstop.

- Virksomhederne står også overfor en trussel fra afpresning, hvor de kriminelle ikke krypterer, men stjæler data og truer med at lække følsomme informationer.

- I deres forsøg på at afpresse virksomhederne udstiller de kriminelle aktører ofte deres ofre offentligt.

Kriminelle aktører angriber produktionsvirksomheder

Center for Cybersikkerhed (CFCS) vurderer, at truslen fra cyberkriminalitet, herunder ransomware-angreb rettet mod danske produktionsvirksomheder, er **MEGET HØJ.**

Truslen udspringer primært af de kriminelle aktørers kapacitet til og intention om at udføre målrettede ransomware-angreb mod europæiske produktionsvirksomheder, herunder virksomheder i Danmark. CFCS har kendskab til, at flere danske produktionsvirksomheder har været ramt af ransomware i 2023.

Da ransomware-aktører angriber opportunistisk, ser man angreb på tværs af industrier, hvor produktion indgår. Produktionsvirksomheder findes i alle samfunds-sektorer, og de kan varetage samfundskritiske funktioner såsom produktionen af fødevarer og medicin. Fælles for dem er, at de fremstiller et fysisk produkt gennem flere processer, og at produktionen af varen kan blive forstyrret eller stoppet af et ransomware-angreb. Et ransomware-angreb kan få konsekvenser, der rækker ud over virksomheden, hvis den f.eks. producerer varer, der er kritiske for samfundet.

Det er specielt angreb fra organiserede ransomware-as-a-service (RaaS) grupper, der dominerer trusselslandskabet. Når man ser på typerne af produktionsvirksomheder, der bliver ramt af ransomware-angreb, lader det ikke til, at aktørerne skelner til, hvorvidt virksomhedernes varer er kritiske for samfundet eller ej. RaaS-gruppen LockBit 3.0 har f.eks. i 2023 taget æren for angreb på både det svenske bryggeri Åbro Bryggeri og den østrigske fabrikant af brandbiler og brandbekæmpende udstyr Rosenbauer.

RaaS: Specialiserede cyberkriminelle samarbejder om udbyttet

Ransomware-as-a-service (RaaS) er en kriminel forretningsmodel, der minder om den platformsøkonomi, som findes på legale markeder.

Bagmændene udvikler ransomwaren og tilbyder den som en service til andre kriminelle partnere, der udfører angrebene hos ofrene. Løsesummerne sendes ofte direkte til bagmændene, der sender en del af beløbene tilbage til partnerne.

Produktionsvirksomheder er et attraktivt mål for ransomware-aktører

RaaS-gruppernes første mål er at opnå indledende adgang til en organisation. Det sker ofte gennem en bredere kampagne, f.eks. phishing-angreb eller kompromitteringer på baggrund af sårbarhedsscanninger, der ikke er målrettet et specifikt offer eller en bestemt industri. Efter den indledende adgang er opnået, målretter grupperne deres indsats mod organisationer, som de forventer kan og vil betale en høj løsesum.

Produktionsvirksomheder er et attraktivt mål for ransomware-aktører, fordi virksomhederne ofte har en høj omsætning og derfor kan betale en stor løsesum til hackerne.

Hackerne kan også have en formodning om, at produktionsvirksomheder er mere villige til at betale løsesummen, da et driftsstop som følge af et angreb kan få store økonomiske konsekvenser for virksomheden.

Foto: Pool/Shutterstock/Ritzau Scanpix

USA: skærpet fokus på truslen fra ransomware

Efter ransomware-angrebene i 2021 mod bl.a. olieselskabet Colonial Pipeline og fødevare-producenten JBS satte de amerikanske myndigheder hårdt ind mod truslen fra ransomware-aktører. Ransomware-angreb kan nu efterforskes som en trussel mod den nationale sikkerhed på samme måde, som det er tilfældet med truslen fra terror.

Indsatsen mod cyberkriminelle er fortsat en prioritet for myndighederne i USA. I slutningen af august 2023 gennemførte FBI en internationalt koordineret operation mod malware-varianten Qakbot. Qakbot blev bl.a. brugt i ransomware-angreb til eksfiltrering af data fra ofre. Adgange til enheder kompromitteret med Qakbot blev hyppigt solgt på kriminelle fora.

Ransomware-angreb kan få konsekvenser for de operationelle processer

IT- og OT-systemer (operativ teknologi) kobles ofte sammen i moderne produktionsmiljøer for at kunne imødegå efterspørgslen på et givent produkt. Deling af data fra forskellige systemer i produktionsmiljøerne kan dog samtidigt gøre virksomhederne mere sårbare overfor angreb, der kan påvirke deres produktion og dermed deres kerneforretning.

På trods af at ransomware typisk er designet til at kryptere klassisk IT-infrastruktur, kan et angreb stadig påvirke en virksomheds OT. Kryptering som følge af et ransomware-angreb kan ramme de IT-systemer, der kontrollerer virksomhedens OT, og derved føre til et produktionsstop, uden at angrebet direkte omfatter selve OT-systemerne.

Et ransomware-angreb kan også føre til et produktionsstop, hvis virksomheden selv lukker ned for systemerne, der styrer produktionen. Det sker typisk, hvis der er frygt for, at de kriminelle kan bevæge sig videre i virksomhedens netværk. Nedlukning blev eksempelvis brugt som forsvarsmekanisme, da Norsk Hydro, der bl.a. producerer aluminium, blev ramt af et angreb i 2019, og da fødevareproducenten Dole blev ramt i februar i år.

Uanset om et produktionsstop sker som følge af selve ransomwaren eller en selvvalgt nedlukning af virksomhedens systemer, kan de økonomiske konsekvenser være betydelige.

Selvvalgt driftstop i kampen mod hackerne

Norsk Hydro, en af verdens største aluminiumsproducenter, var offer for et ransomware-angreb mod virksomhedens IT-systemer. I en forebyggende handling lukkede de produktionen, da de opdagede angrebet, hvilket tvang virksomheden til at overgå til manuel produktion. De finansielle konsekvenser af angrebet skønnes til op mod 500 mio. danske kroner for Norsk Hydro.

Den 22. februar 2023 annoncerede fødevareproducenten Dole, at de var ramt af et ransomware-angreb. Som følge af angrebet lukkede Dole midlertidigt flere af deres fabrikker i Nordamerika og satte samtidigt al distribution på pause. Det gjorde bl.a., at der i nogle amerikanske supermarkeder var mangel på visse Dole-produkter i over en uge efter angrebet.

RaaS-grupper kan bruge flere afpresningsmetoder i jagten på løsesummen

Selvom et ransomware-angreb typisk inkluderer en kryptering af data og systemer, har nogle RaaS-grupper videreudviklet angrebsmetoden. Et eksempel er den cyber-kriminelle gruppe Karakurt, der stjæler offerets data, men ikke krypterer data eller systemer. Derefter truer gruppen offeret med at lække eller sælge det stjålne data, hvis løsesummen ikke betales. For RaaS-grupperne kan datatyveri og afpresning uden kryptering være attraktiv, da det kræver mindre arbejde og færre tekniske færdigheder.

Selvom virksomheden i et sådant angreb kan slippe for et pludseligt produktionsstop, kan lækket data stadig gøre skade på virksomheden. Eksfiltreret data kan både indeholde følsomme personoplysninger, sensitive kundedata eller forretnings-hemmeligheder, som kan skade virksomhedens konkurrenceevne og omdømme, hvis data bliver lækket eller solgt. Hvor data, der er blevet krypteret, kan genskabes fra en god backup, så er der derimod ikke meget at gøre, hvis data først er blevet eksfiltreret fra virksomhedens systemer. Derudover kan det være nødvendigt at lukke dele af produktionen ned, mens man sikrer sig, at hackerne ikke længere har adgang til systemerne.

Offentlig udskamning bruges som afpresningsteknik
I modsætning til mere traditionelle former for kriminalitet, hvor de kriminelle oftest ikke ønsker at blive opdaget, annoncerer de organiserede RaaS-aktører ofte deres angreb meget direkte overfor ofrene og til tider omverdenen. Det gør grupperne typisk på to måder.

Den første sker i den sidste fase af angrebet, når offerets systemer og data er krypteret eller stjålet af de kriminelle. Her efterlader hackerne ofte en note med instruktioner og krav om betaling af løsesummen. Nogle RaaS-grupper efterlader instruktioner til, hvordan offeret kan kommunikere direkte med dem.

Den næste og mere offentlige måde, hvorpå hackerne annoncerer et angreb, sker via deres dedicated leak site (DLS). En DLS er en hjemmeside, der er styret af ransomware-aktørerne. Sidens formål er at udstille de ofre, som aktørerne angriber. Hvis en virksomhed nægter at betale løsesummen eller ikke overholder tidsfristen for betaling, er der flere ransomware-grupper, der offentliggør navnet på virksomheden på gruppens DLS. Hvis hackerne har stjålet data, kan de også vælge at lække det samtidigt. Aktørens motiv er at udstille offeret og på den måde skræmme fremtidige ofre til at betale løsesummen. DLS kaldes også for en *victim shaming blog*.

De kriminelle aktører bruger offentlig udstilling, fordi det kan skade en virksomheds omdømme og forretning, hvis det bliver offentligt kendt, at virksomheden har været udsat for et ransomware-angreb. Hertil kan en offentliggørelse af sensitive kunde- eller medarbejderdata risikere at medføre bødestraf til virksomheden.

Ransomware-aktører bruger kreative midler for at udskamme deres ofre til betaling af løsesummen

Kriminelle aktører vil gå langt for at lægge pres på virksomhederne, så de kan få udbetalt løsesummen for det krypterede eller stjålne data.

Et eksempel er en affilieret til RaaS-gruppen ALPHV, der efter et ransomware-angreb kommenterede på et offers LinkedIn-opslag med et link til noget af det eksfiltrerede data. Linket blev i kommentaren efterfulgt af en trussel om offentliggørelse af resten af det stjålne data, hvis offeret ikke kontaktede gruppen og forhandlede om en løsesum.

RaaS-grupper har også ringet og truet medarbejdere, printet ransom-notes på printere i det kompromitterede netværk samt truet med overbelastningsangreb mod ofrenes hjemmesider, som led i deres afpresning. Overbelastningsangreb kaldes også for DDoS (Distributed Denial-of-Service).

Trusselsniveauer

Forsvarets Efterretningstjeneste bruger følgende trusselsniveauer.

INGEN	Der er ingen tegn på en trussel. Der er ingen aktør, der både har kapacitet til og intention om angreb/skadelig aktivitet.
LAV	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men enten er kapaciteten eller intentionen eller begge dele begrænset.
MIDDEL	En eller flere aktører har kapacitet til og intention om angreb/skadelig aktivitet. Men der er ikke indikationer på specifik planlægning af angreb/skadelig aktivitet.
HØJ	En eller flere aktører har kapacitet til og foretager specifik planlægning af angreb/skadelig aktivitet, eller har allerede gennemført eller forsøgt angreb/skadelig aktivitet.
MEGET HØJ	Der er enten oplysninger om, at en eller flere aktører iværksætter angreb/skadelig aktivitet, herunder oplysninger om tid og mål, *eller* en eller flere aktører iværksætter kontinuerligt angreb/skadelig aktivitet.

Et givent trusselsniveau er udtryk for FE's vurdering af aktørers intention, kapacitet og aktivitet på baggrund af de tilgængelige oplysninger.