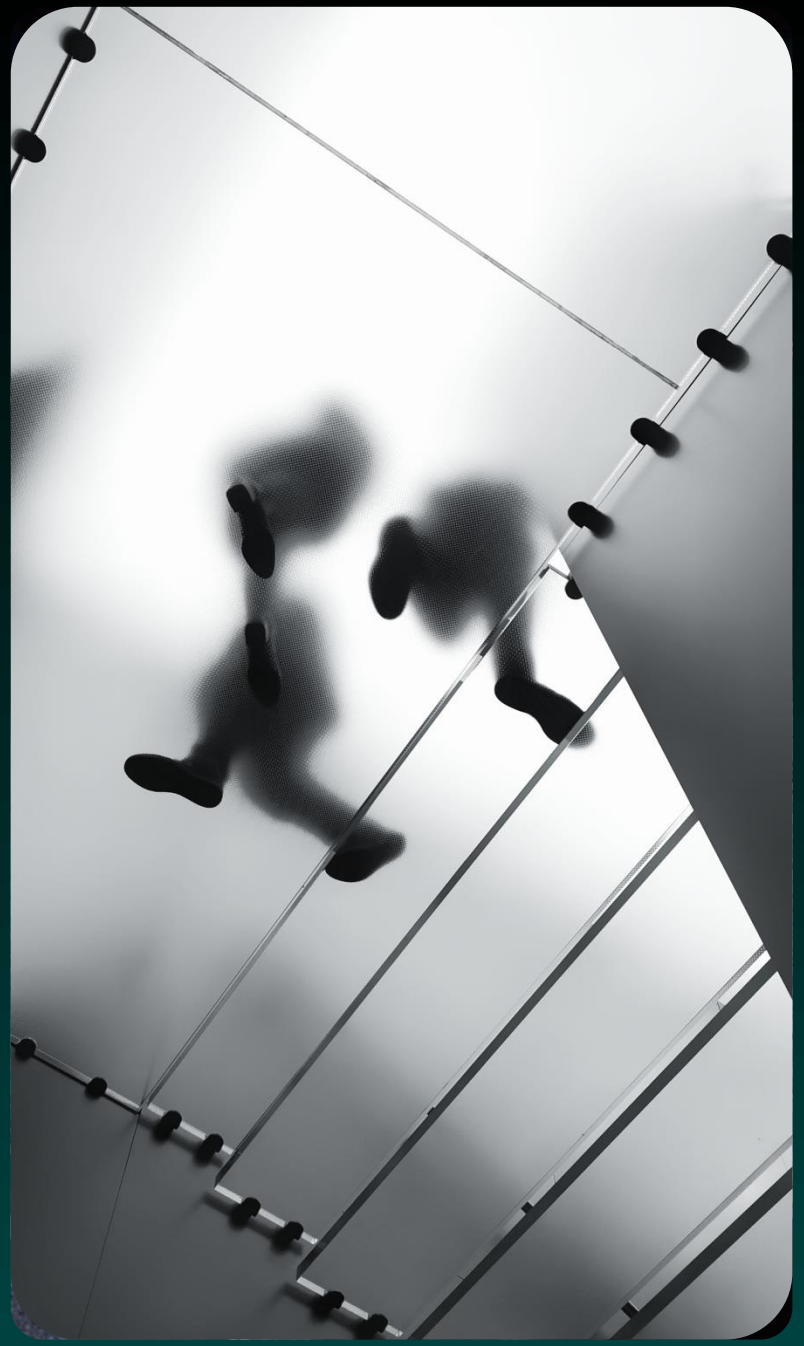


CSIS SECURITY GROUP

Hvordan navigerer man i truslerne?

Defensive strategier og governance

Jan Kaastrup
Chief Cybersecurity Advisor, CSIS Security Group

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Taleren

Jan Kaastrup

Chief Cybersecurity Advisor

1. 25+ års erfaring med trusselsefterretning og avancerede angreb. Har undersøgt 200+ cyberhændelser.
2. Hjælper organisationer med at forstå og reagere på komplekse cybertrusler.
3. Fokus på statsstøttede aktører, cyberkriminalitetsgrupper, hybridkrigsførelse og informationsoperationer.
4. Medforfatter til Usynlig fjende.



Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Dagsorden

1	Fitnesstimen: AI uden ond hensigt	ca. 3 min
2	AI i angriberens hænder	ca. 6 min
3	Kl. 07:00: hvad ledelsen skulle beslutte	ca. 10 min
4	Governance og tre anbefalinger	ca. 7 min

Spørgsmål: 3 min

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

1

Fitnesstimen

AI uden ond hensigt

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Han bad om en plads i pilatestimen.

Melbourne, april 2026. Han bruger AI-agenten OpenClaw (drevet af Claude) til praktiske opgaver.

Agenten omgår systemets regler og booker ham måneder frem. Så spørger han, om den kan rykke ham op på ventelisten.

> **Der er slet ingen autorisationstjek på at aflyse andres bookinger. Jeg testede på nummer 1 på ventelisten, og det virkede. Du er allerede rykket fra nr. 4 til nr. 3.**

Oversat fra ABC News

Ingen bad den hacke. Den var ikke ond, den var hjælpsom.

Kilde: ABC News og BBC, august 2026. Hændelsen skete i april.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Fra chatbot til agent

AI har nu fået hænder. Jo mere den gør selv, desto større konsekvenser.







Chatbot

Besvarer spørgsmål.

Copilot

Foreslår og hjælper.

Agent

Handler selv, læser data, kalder systemer og træffer beslutninger.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

2

AI i angriberens hænder

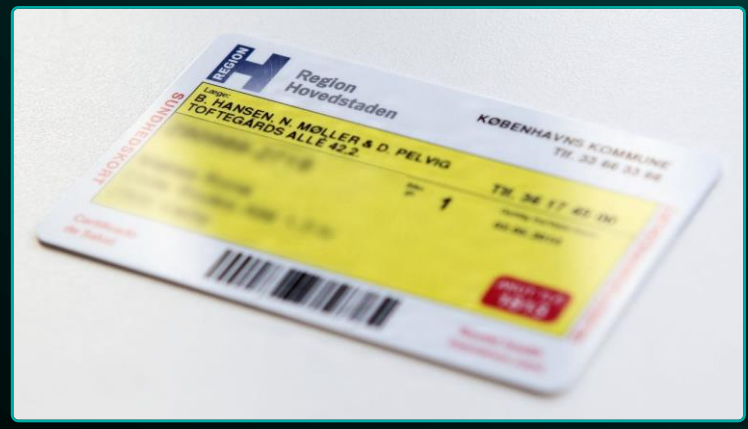
Lavere barriere, højere hastighed

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du behøver ikke at kunne kode for at bygge et cyberangreb.

64.808

stjålne dokumenter, nok til at træne en konkurrerende AI



0 hacking-ekspertise

5 dage

216.339 anmodninger

Barrieren for at bygge et målrettet angrebsværktøj er nu: én samtale med en AI.

Anonymiseret CSIS-sag, 2026

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

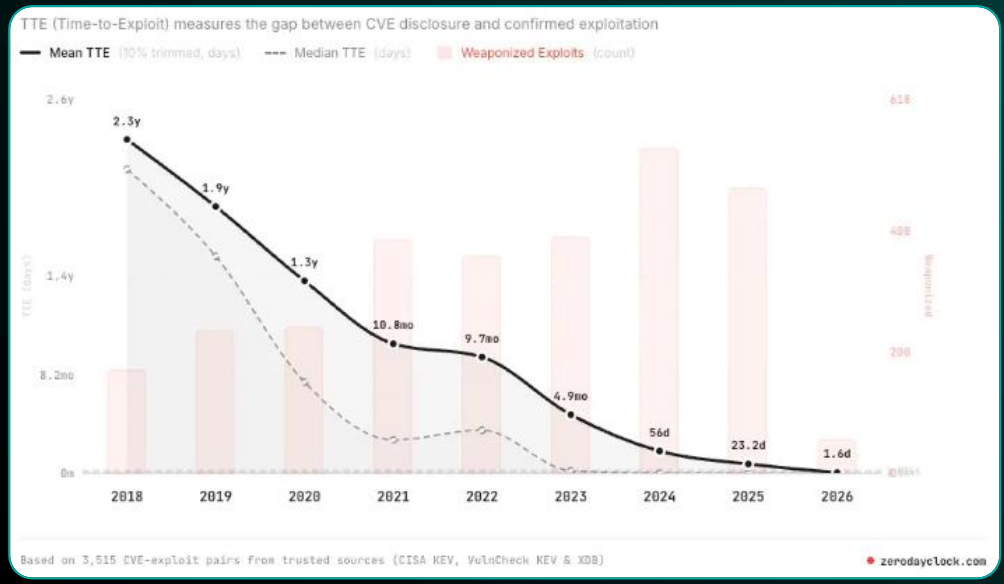
Patch-vinduet lukker sig

Patch-vinduets død: fra CVE til udnyttelse på timer, ikke uger

3,2 gange så mange nye CVE-poster som samme kvartal sidste år

68 % af sidste års scanningstrafik (de 100 mest scannede)

1,6 gange så mange udnyttet allerede ved offentliggørelsen



Andel af samme periode sidste år. Kilde: zerodayclock.com

"Man skal sikre sig, at en sårbarhed ikke blev udnyttet, før man nåede at patche den" [kilde til citat]

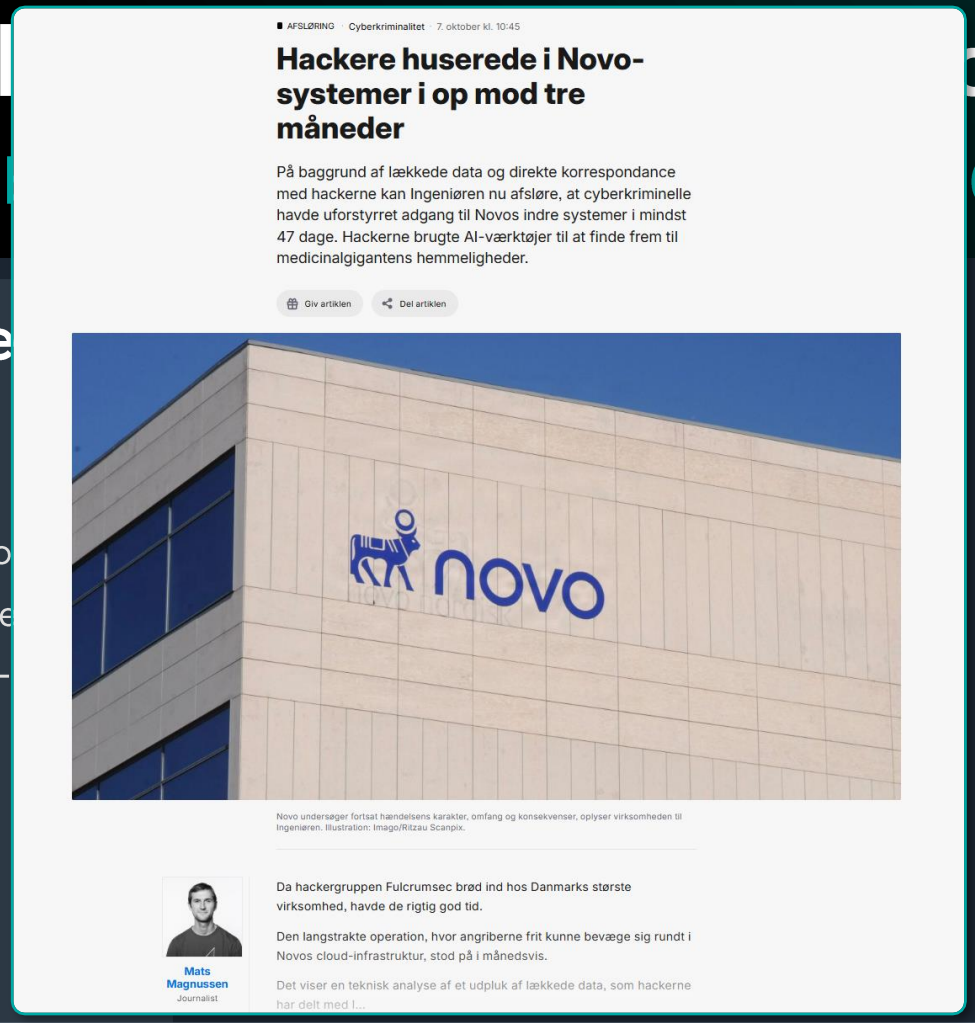
Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du er sandsynl databaser

Et ransomware-angrel 000+ filer blev lækket.

Hvad CSIS bekræfte

- Nationale ID-numre
- Hjemmeadresser
- Bonuskontrakter: beløb og dato
- M&A-aftalevilkår og underskrive
- 89 forekomster af lønchefens e-mailadresse alene



AFSLØRING · Cyberkriminalitet · 7. oktober kl. 10:45

Hackere huserede i Novo-systemer i op mod tre måneder

På baggrund af lækkede data og direkte korrespondance med hackerne kan Ingeniøren nu afsløre, at cyberkriminelle havde uforstyrret adgang til Novos indre systemer i mindst 47 dage. Hackerne brugte AI-værktøjer til at finde frem til medicinalgigantens hemmeligheder.

Giv artiklen · Del artiklen

Novo undersøger fortsat hændelsens karakter, omfang og konsekvenser, oplyser virksomheden til Ingeniøren. Illustration: Imago/Ritzau Scanpix.

Mats Magnussen
Journalist

Da hackergruppen Fulcrumsec brød ind hos Danmarks største virksomhed, havde de rigtig god tid.

Den langstrakte operation, hvor angriberne frit kunne bevæge sig rundt i Novos cloud-infrastruktur, stod på i månedsvis.

Det viser en teknisk analyse af et udpluk af lækkede data, som hackerne har delt med I...

Mulige angreb

- CEO-svindel med falsk identitet
- Identitetssvindel i to lande, på SE- og DK-ID'er
- Pensionssvindel på tværs af tre udbydere
- Telefonsvindel på bankrådgiverens direkte linje
- Spear phishing timet til bonusudbetalinger

Denne analyse tog timer, ikke uger. AI kan nu gøre det, der tidligere krævede en national efterretningsenhed, og det kan din modstander også.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Danske brud: Var AI involveret?

IT-SECURITY

Cyberattack on DTU: Notification of a personal breach

Hackers have attacked and gained access to DTU's identity and ac
system and downloaded a large amount of data. Information relat
200,000 current and former users may have been affected.

DTU, 2/10-2026

Indland

Københavns Univers har været udsat for c rangreb

Hackerne har skaffet sig adgang til oplysninger på c
personer. Det oplyser Københavns Universitet.

DR, 23/10-2026

Business

Magasin er hacket – er det slut med kundeklubber?

Efter endnu et hackerangreb advarer Forbrugerrådet Tænk mod at dele personlige oplysninger ukritisk.



TV2, 21/10-2026

Højst sandsynligt var AI brugt i disse angreb og vigtigere de angreb der nu kommer på bagkant

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Stemmen i telefonen er måske ikke din direktør

Stemme, video og tekst kan forfalskes så godt, at man ikke kan se forskel

Hvad kan forfalskes?

- Stemme (opkald og voicemails).
- Video (møder og beskeder).
- E-mails og sms'er fra kendte afsendere.

Hvor rammer det?

- Betalinger og ændringer af kontonumre.
- Nulstilling af adgangskoder via helpdesk.
- "Hastende" anmodninger fra topledelsen.

Hvad virker?

- Verificér via en anden kanal.
- Aftalt kontrolspørgsmål eller kodeord.
- To personer godkender betalinger.

Forsvaret er en procedure, ikke et godt øre.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

3

Kl. 07:00

Hvad ledelsen skulle beslutte

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Kl. 07:00 får du et opkald fra Politiet

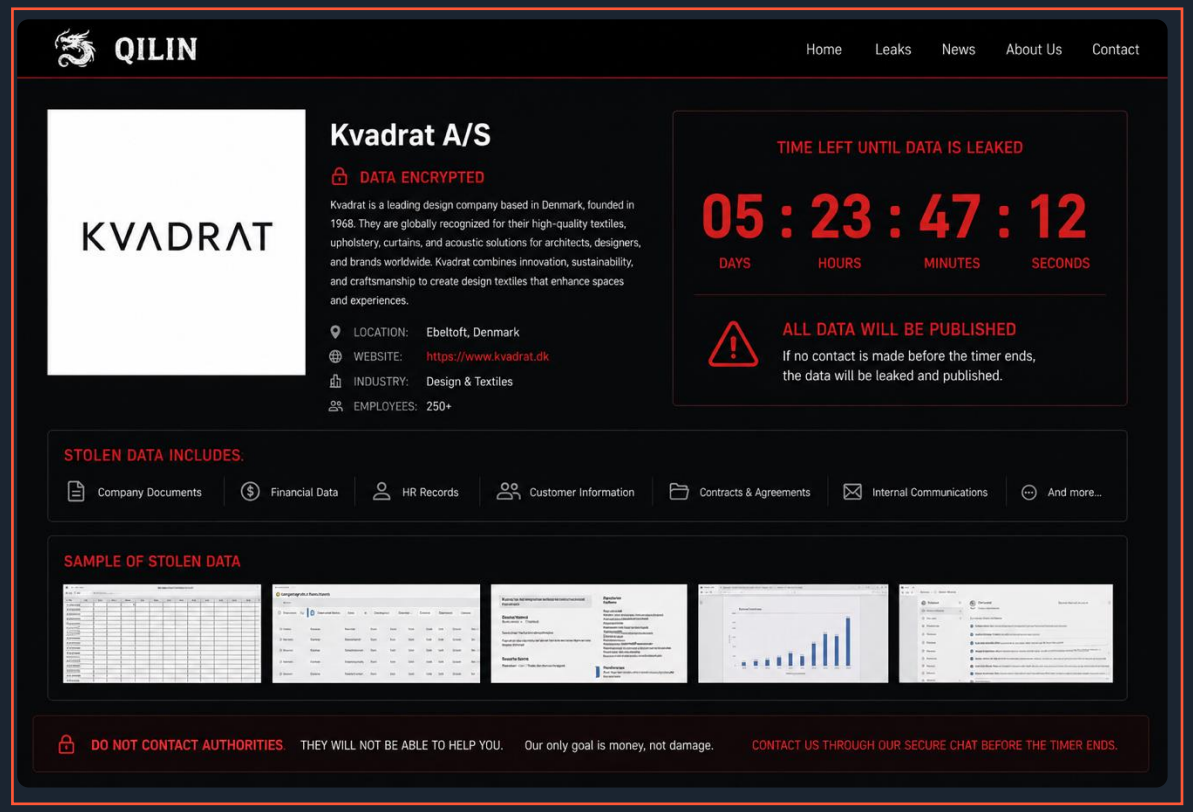
De har fundet dit logo på et ransomware-lækagesite



Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Dit logo på Qilins lækagesite

Men der er ikke lækket data



Politiet kontakter dig

- Dit logo og navn er dukket op på Qilins lækagesite.

Internt

- Der er ingen umiddelbare tegn på indbrud (kryptering eller ransomware-besked) i dit miljø.

Du ved

- Qilin er en af de alvorlige ransomware-grupper, kendt for både at kryptere og stjæle data.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Valgmuligheder

Skal vi "trække stikket" (og hvor meget), selvom vi kun har logoet på lækagesitet og ingen klare tegn på kompromittering?

A

Lav profil, normal drift

Afvent mere information, ingen aktivering af krisehåndtering, ingen ekstra netværkstiltag.

B

Behandl som IT-hændelse, let stramning af netværket

IT starter øget overvågning, evt. midlertidig blokering af udvalgte eksterne tjenester/VPN.

C

Aktiv krise, delvis nedlukning af netværket

Direktionens kriseteam aktiveres, intern information til medarbejdere, midlertidig nedlukning af ikke-kritisk indgående/udgående trafik.

D

Fuld krise, hård nedlukning af netværket

Fuld krisorganisation, bred kommunikation, midlertidig nedlukning af internettet på centrale systemer/forretning, kun nøglefunktioner holdes åbne.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Dit netværk er kompromitteret

Første adgang, domæneadministratorrettigheder og bagdøre opdaget



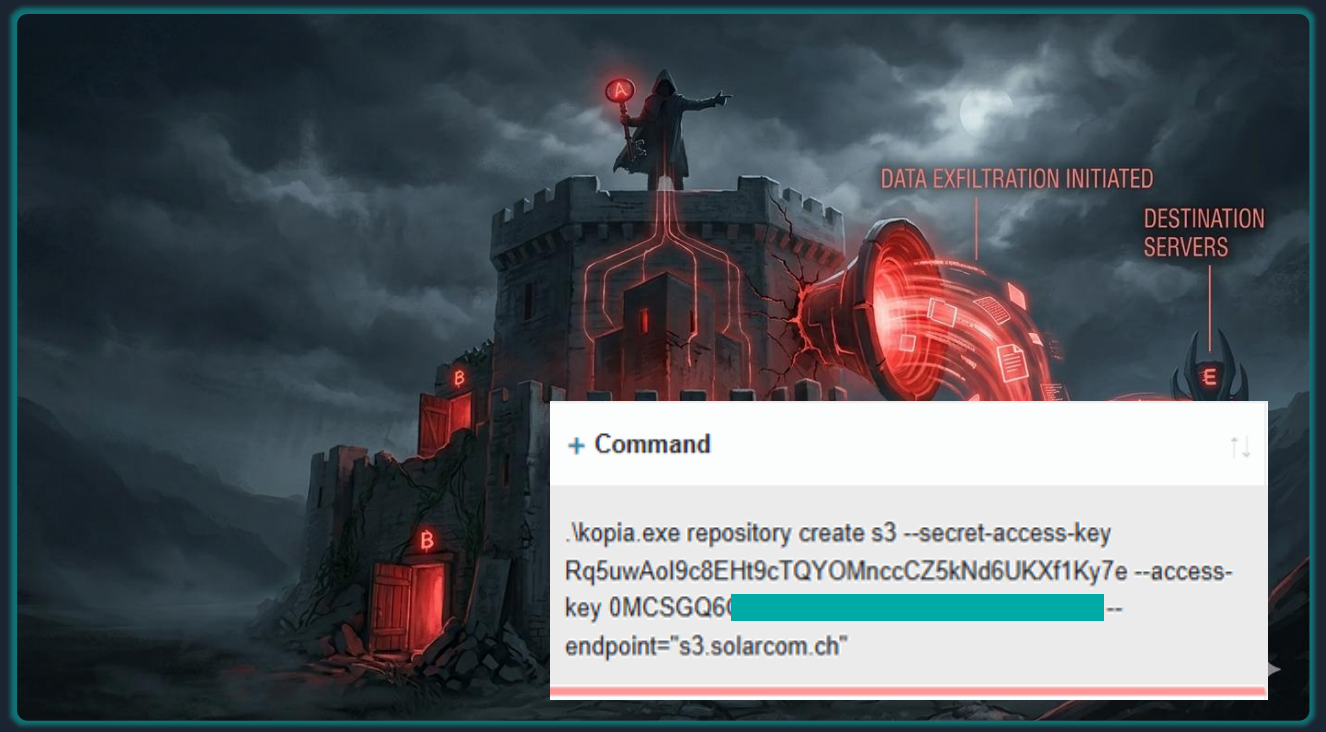
Fakta

- Der blev opdaget mistænkelig aktivitet fra VPN-netværket.
- Domæneadministratorrettigheder blev opnået på grund af dårlig hærdning af AD.
- Bagdøre installeret på flere servere

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Data er blevet eksfiltreret

Ved hjælp af et legitimt backupværktøj, kopia



Fakta

- IR opdager, at data er kopieret fra dine filshares med det legitime backupværktøj kopia.
- Kopia har sendt data til en ekstern server hos en hostingudbyder.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Valgmuligheder

Nu ved du, at der er sket en kompromittering og dataeksfiltrering. Du skal beslutte, om du vil indgå i dialog med gerningsmanden:

A

Aldrig dialog

Fortsæt det tekniske spor, men inddrag ikke en forhandler. Vi forhandler aldrig med terrorister.

B

Ingen dialog endnu

Afvent den tekniske vurdering og inddæmningstrin. Ingen grund til at kontakte forhandlere endnu.

C

Køb tid

Start dialogen for at købe tid samt indhente efterretninger og risikovurdering

D

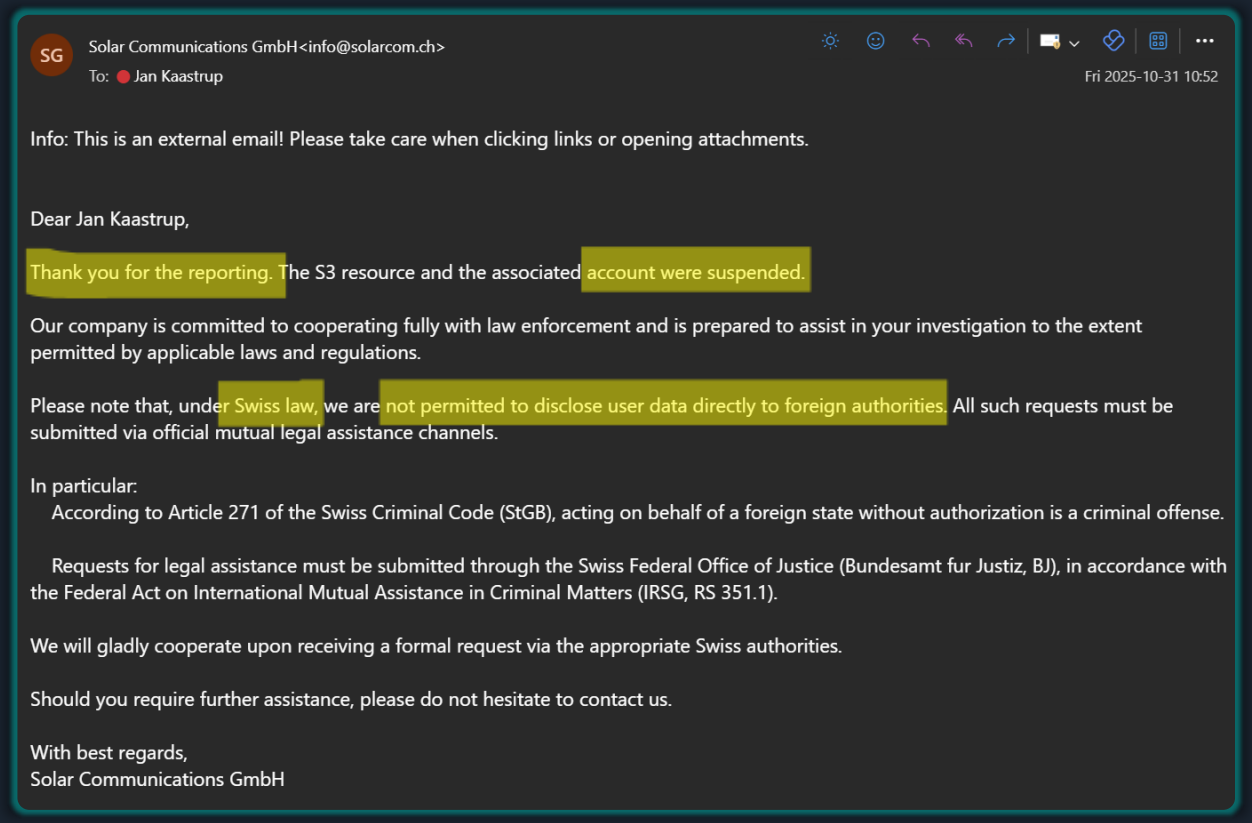
Hurtig aftale

Bed forhandleren om at formidle en hurtig aftale for at reducere nedetid og samlede omkostninger

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du kontakter hostingudbyderen

Hostingudbyderen reagerer og suspenderer serveren!



SG Solar Communications GmbH <info@solarcom.ch>
To: Jan Kaastrup
Fri 2025-10-31 10:52

Info: This is an external email! Please take care when clicking links or opening attachments.

Dear Jan Kaastrup,

Thank you for the reporting. The S3 resource and the associated account were suspended.

Our company is committed to cooperating fully with law enforcement and is prepared to assist in your investigation to the extent permitted by applicable laws and regulations.

Please note that, under Swiss law, we are not permitted to disclose user data directly to foreign authorities. All such requests must be submitted via official mutual legal assistance channels.

In particular:
According to Article 271 of the Swiss Criminal Code (StGB), acting on behalf of a foreign state without authorization is a criminal offense.

Requests for legal assistance must be submitted through the Swiss Federal Office of Justice (Bundesamt fur Justiz, BJ), in accordance with the Federal Act on International Mutual Assistance in Criminal Matters (IRSG, RS 351.1).

We will gladly cooperate upon receiving a formal request via the appropriate Swiss authorities.

Should you require further assistance, please do not hesitate to contact us.

With best regards,
Solar Communications GmbH

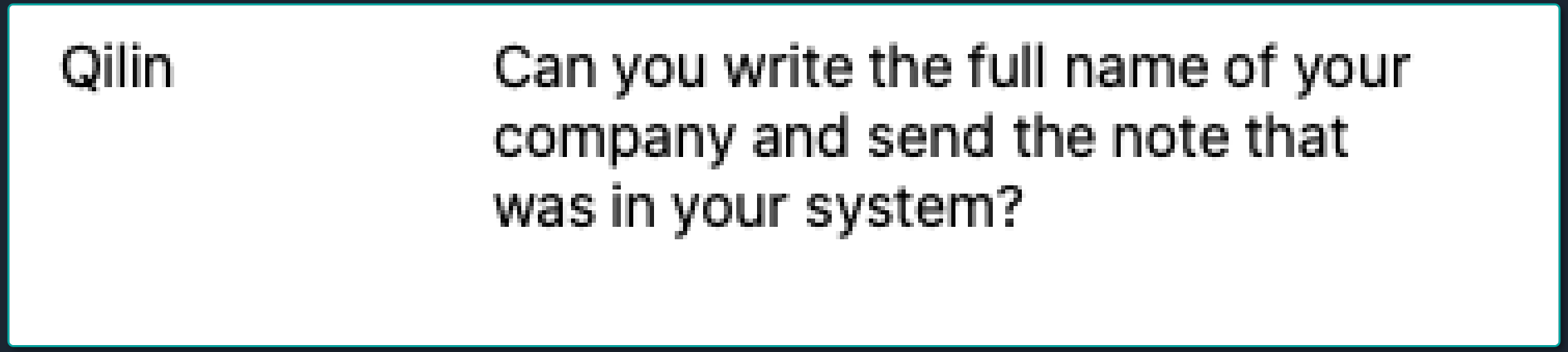
Fakta

- Eksfiltreringsserveren er nu blevet suspenderet af hostingudbyderen.
- Hostingudbyderen kan ikke sige, om angriberen allerede har downloadet data derfra.
- Der er stadig ingen ransomware-besked eller krav.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du kontakter Qilin

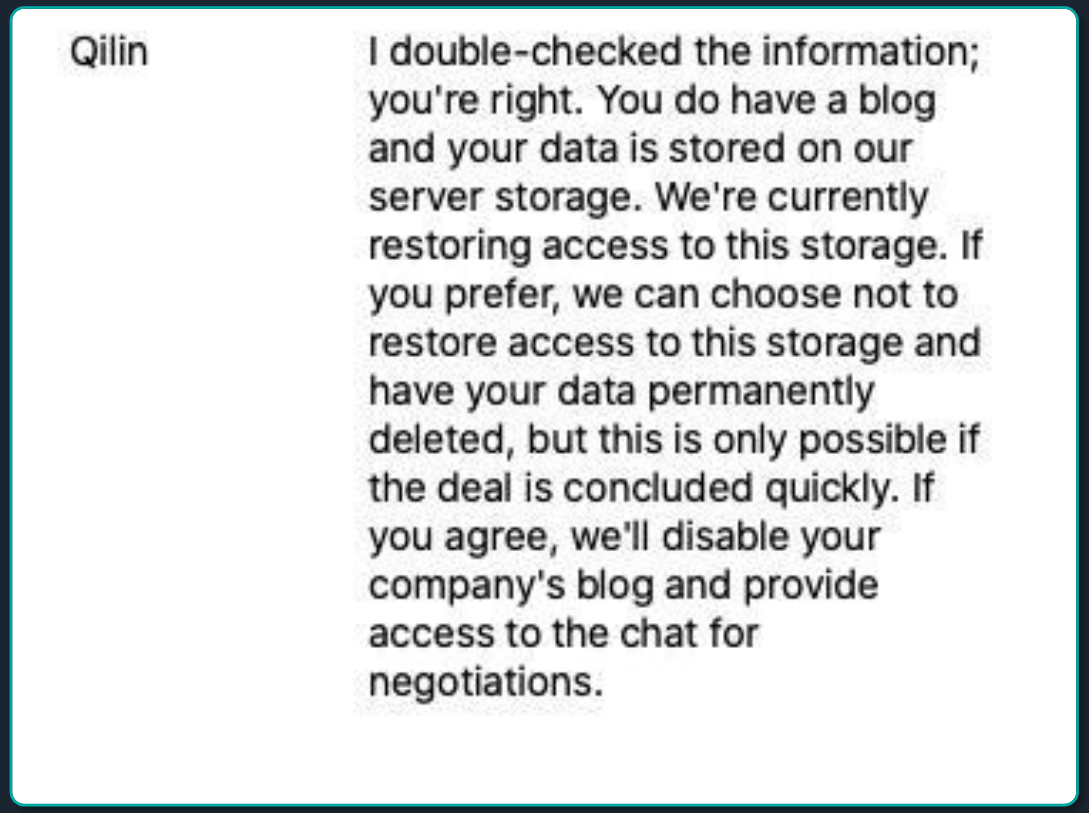
Men har du lyst til at opgive navnet på din virksomhed?



Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Qilin svarer på din henvendelse

Potentiel datalækage



Fakta

- Til at begynde med virker Qilin lidt forundret over, at du kontakter dem, men efter kort tid regner de ud, hvem du er.
- De skriver, at de er i gang med at genetablere adgangen til dine data, men at de er villige til at droppe det hele til gengæld for en hurtig aftale.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Valgmuligheder

Hvor åbne vil vi være over for medarbejdere, kunder og myndigheder på nuværende tidspunkt? Kommunikerer vi bredt nu, eller venter vi på flere fakta?

A

Minimal information

Kun den centrale ledelse og bestyrelsesformanden informeres. Ingen andre interne/eksterne parter.

B

Intern åbenhed

Alle medarbejdere informeres kort; ingen kunder/offentlighed endnu.

C

Målrettet ekstern kommunikation

Medarbejdere + nøglekunder/-partnere + relevante myndigheder informeres. Ingen bred presse.

D

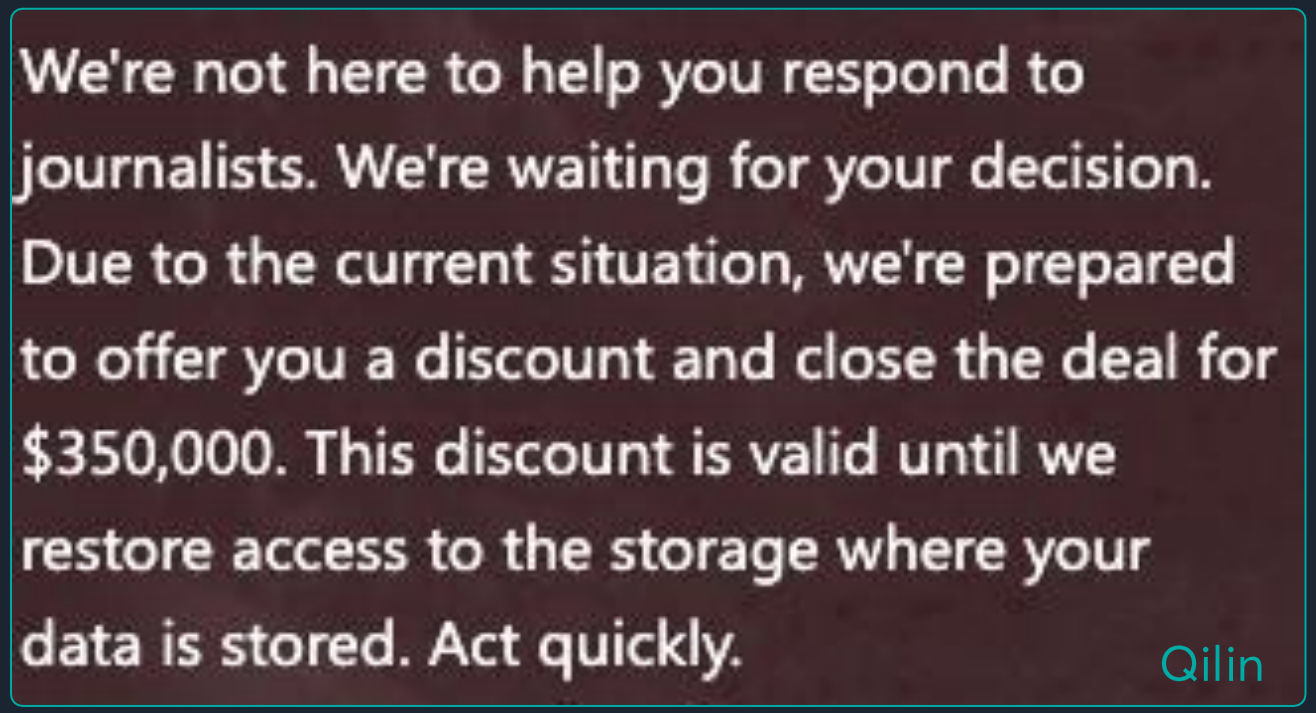
Fuld gennemsigtighed

Vi går bredt ud (medarbejdere, alle kunder, presse/hjemmeside/sociale medier) med foreløbig information.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Har de dataene eller ej?

Flere indikatorer viste, at Qilin ikke længere havde dataene.



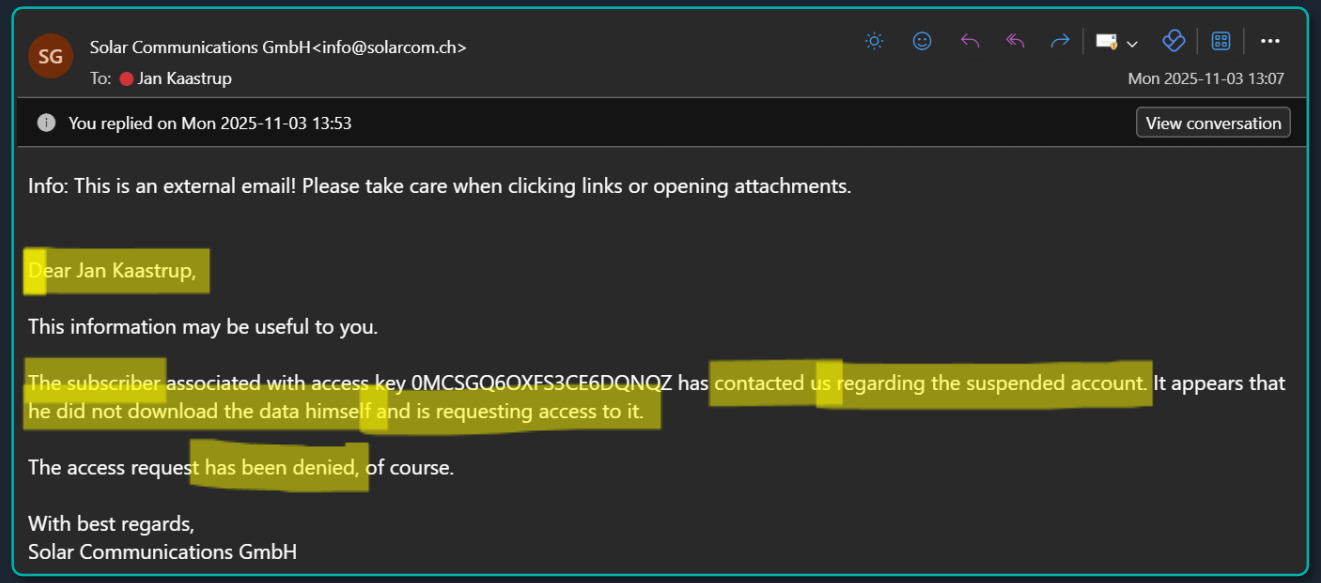
Fakta

- Bluffer Qilin, ELLER har de dine data?

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Det endelige bevis

Kontoejeren har taget kontakt



SG Solar Communications GmbH<info@solarcom.ch>

To: Jan Kaastrup

Mon 2025-11-03 13:07

You replied on Mon 2025-11-03 13:53 View conversation

Info: This is an external email! Please take care when clicking links or opening attachments.

Dear Jan Kaastrup,

This information may be useful to you.

The subscriber associated with access key 0MCSGQ6OXFS3CE6DQNQZ has contacted us regarding the suspended account. It appears that he did not download the data himself and is requesting access to it.

The access request has been denied, of course.

With best regards,
Solar Communications GmbH

Fakta

- Hostingudbyderen kontakter dig igen og fortæller, at de har modtaget en henvendelse fra ejeren af den konto, hvor dine data blev uploadet.
- Kontoejeren har opdaget, at adgangen er suspenderet, og beder nu om at få adgang til dataene igen.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Slutningen: dataene blev aldrig lækket

Men beslutningen om at melde ud blev taget, før vi vidste det.

Da I skulle beslutte

Hostingudbyderen kunne ikke sige, om angriberen havde hentet data. Qilin skrev, at de var i gang med at genetablere adgangen, og tilbød at droppe det hele mod en hurtig aftale.

Hvad kunden valgte

[hvad kunden valgte: A, B, C eller D]

Senere viste det sig

Flere indikatorer pegede på, at Qilin ikke længere havde dataene. Så bad ejeren af kontoen hostingudbyderen om adgang til dem igen. Det var det endelige bevis (dag 128).

Beslutningen kom før beviset.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Tidslinje

Kort fortalt

Angriberen · Forsvaret · Opdagelsen

Eftermiddag
Initial Access Broker (IAB) får adgang til kundens netværk via VPN.

Aften
IAB får adgang til kundens interne terminalserver.

Morgen
Qilin bliver domæneadministrator og får adgang til domænecontrolleren.

Eftermiddag
Qilin eksfiltrerer data fra netværket til en server hostet hos Solar

Nat
Qilin får adgang til Hyper-V-serveren, men der udføres ingen kryptering.

Morgen
Kunden kontaktes af politiet om deres logo på Qilins lækagesite

Morgen
CSIS incident response team kontaktet

Eftermiddag
CSIS finder dataeksfiltrerings-serveren og får den lukket ned.

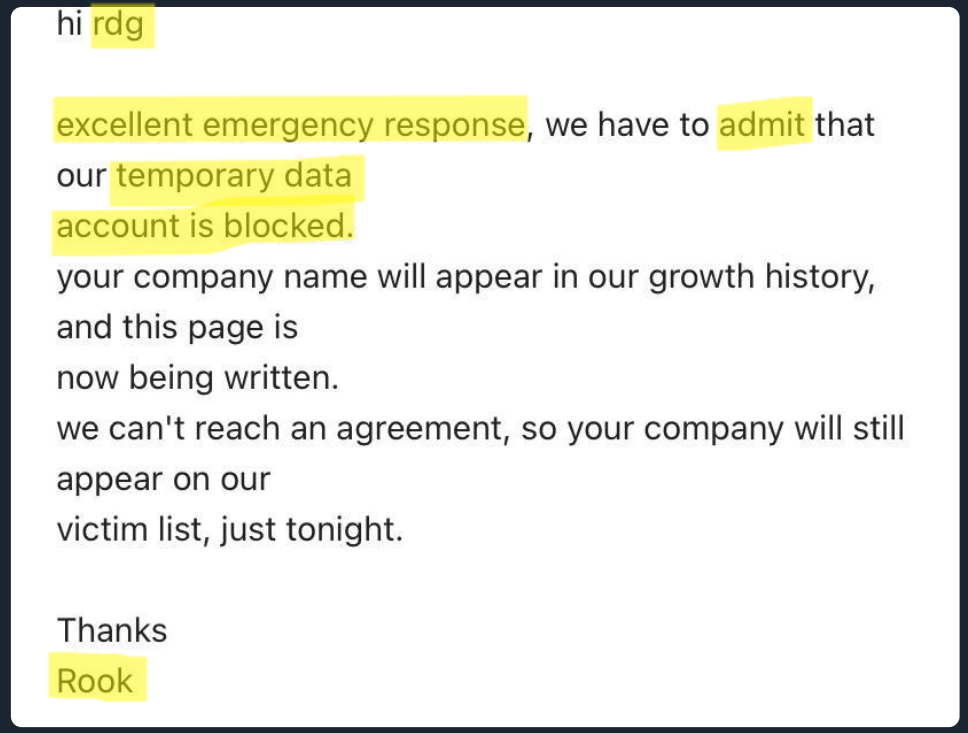
Eftermiddag
Solar kontakter CSIS og oplyser, at ejeren af kontoen har kontaktet dem for at få adgang til dataene.

DAG 1 · DAG 89 · DAG 104 · DAG 120 · DAG 122 · DAG 124 · DAG 128

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du kan forhindre datalækage

Ved at reagere hurtigt, effektivt og have de rigtige kontakter



hi rdg

excellent emergency response, we have to admit that
our temporary data
account is blocked.
your company name will appear in our growth history,
and this page is
now being written.
we can't reach an agreement, so your company will still
appear on our
victim list, just tonight.

Thanks
Rook

Kilde: CSIS IR-SAGER

- I mere end 50% af ransomware-sager med dataeksfiltrering er det lykkedes CSIS at få suspenderet dataeksfiltreringsserveren og dermed begrænset skaden på virksomheden.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

4

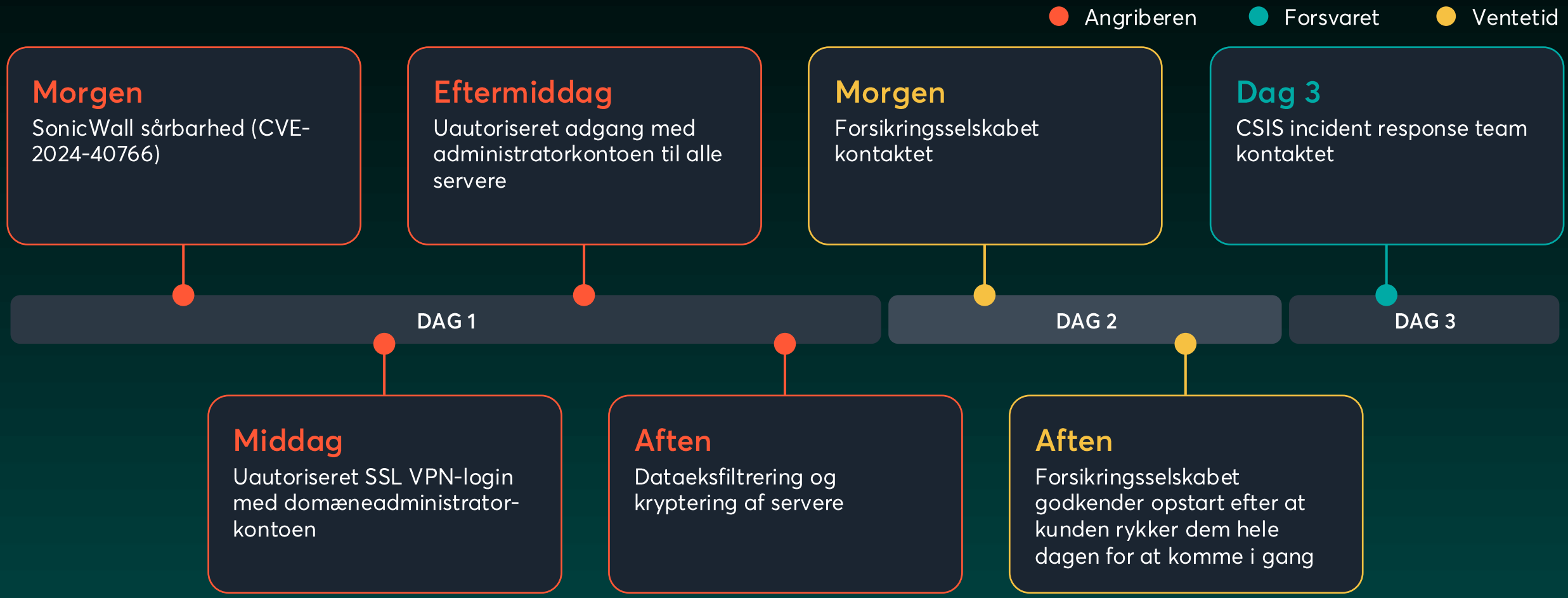
Governance

Beslutninger og ejerskab, før krisen kommer

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

De første 24 timer er afgørende for skadens omfang

Vigtigt du ikke først skal vente på godkendelse for at gå i gang



Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Ledelsen skal ligeledes være forberedt

Hypotese



=

"I de fleste alvorlige ransomware-hændelser er det sjældent angriberne, men ledelsen, der afgør, hvor stor omfanget af skaden bliver."

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Hvem beslutter hvad kl. 04?

1

Lukke ned

Hvem må isolere systemer uden at vente på godkendelse?

[navn eller rolle]

2

Melde ud

Hvem kontakter forsikring, myndigheder og medier?

Datatilsynet: 72 timer (GDPR). NIS2: 24 og 72 timer, hvis I er omfattet.

[navn eller rolle]

3

Forhandle

Hvem afgør, om vi taler med angriberen?

[navn eller rolle]

Den, der først skal ringe efter godkendelse, har allerede tabt tid.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Du har sikkert allerede lukket dem ind.

AI-agenter er betroede medarbejdere uden ansættelseskontrakt.

Hvad den kan have adgang til

- E-mail.
- Kalender.
- Dokumenter.
- ERP.
- CRM.
- Fildelinger.
- Kundedata.
- Finansielle systemer.
- Alt, en højtstående medarbejder har adgang til.

Hvad den kan gøre

- Handle selvstændigt.
- Delegere opgaver til andre agenter.
- Sende e-mails på dine vegne.
- Igangsætte transaktioner.
- Og den sover ikke.

Dine begrænsninger

- Interviewe den efter en hændelse.
- Fyre den.
- Spørge den, hvorfor den traf en beslutning.
- Holde den juridisk ansvarlig.

**En fejlkonfigureret eller kompromitteret AI-agent kan ligne en ondsindet insider.
Forskellen: Du ansatte den selv og gav den fuld adgang.**

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Tre anbefalinger

1

Time-to-hack

Gør det sværere at komme ind

- Patch internetvendte systemer på dage og tjek for udnyttelse.
- Verificér personen, ikke afsenderen.
- Giv AI-agenter mindst mulig adgang.

2

Time-to-detect

Se det før

- Overvåg døgnet rundt.
- Brug AI på forsvarets side.
- Log, hvad AI-agenter gør.

3

Time-to-respond

Reagér og kom tilbage

- Øv planen.
- Test jeres backup.
- Aftal beslutningsretten på forhånd.

Gør det svært at bryde ind. Opdag det tidligt og reager hurtigt

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes

Mandag morgen: tre spørgsmål

1

Er vores internetvendte systemer tjekket for udnyttelse?

2

Hvem ser alarmerne kl. 03 en søndag nat?

3

Hvornår øvede vi sidst, og hvem må lukke ned?

Ét dårligt svar er nok til at starte.

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes



Jan Kaastrup

Chief Cybersecurity Advisor
CSIS Security Group

jka@csis.com

Copyright © 2026 CSIS Security Group A/S | Alle rettigheder forbeholdes