Synology

Beskyt din organisation mod ransomware

Ransomware-angreb forventes at koste organisationer samlet US billion alene i 2023.[1] Det er afgørende med planer for databeskyttelse med hurtige genoprettelsesløsninger for at mindske effekten af ransomware og andre former for cyberkriminalitet.

Date 13. okt 2023

Backup: Den sidste forsvarslinje, når katastrofen rammer

Når data går tabt efter ondsindet sletning eller ændring, giver backupkopier dig mulighed for at gendanne vigtige data og undgå dyr nedetid. Benyt Synologys databeskyttelsesløsninger til at designe en backupstrategi for hele din IT-infrastruktur.

Komplet beskyttelse

Beskyt slutpunkter samt primære backupkopier for at oprette flere sikkerhedsnet til dine data.

Hurtig gendannelse

Reducer nedetid til et minimum, når katastrofen rammer, med funktioner til øjeblikkelig gendannelse.

Uforanderlig lagring

Undgå uautoriserede ændringer af data og snapshots.

Backup uden licens

Tag backup af så mange data, som dit lager tillader, uden begrænsninger eller skjulte gebyrer.

Centraliseret beskyttelse mod ransomware

Konsolider backupkopier fra flåder af arbejdsstationer, servere, virtuelle maskiner og skyprogrammer. Optimer lagerforbruget, og undgå flaskehalse i båndbredden med datadeduplikering og trinvis backupteknologi. https://www.synology.com/dsm/solution/infrastructure

Fysiske arbejdsbelastninger

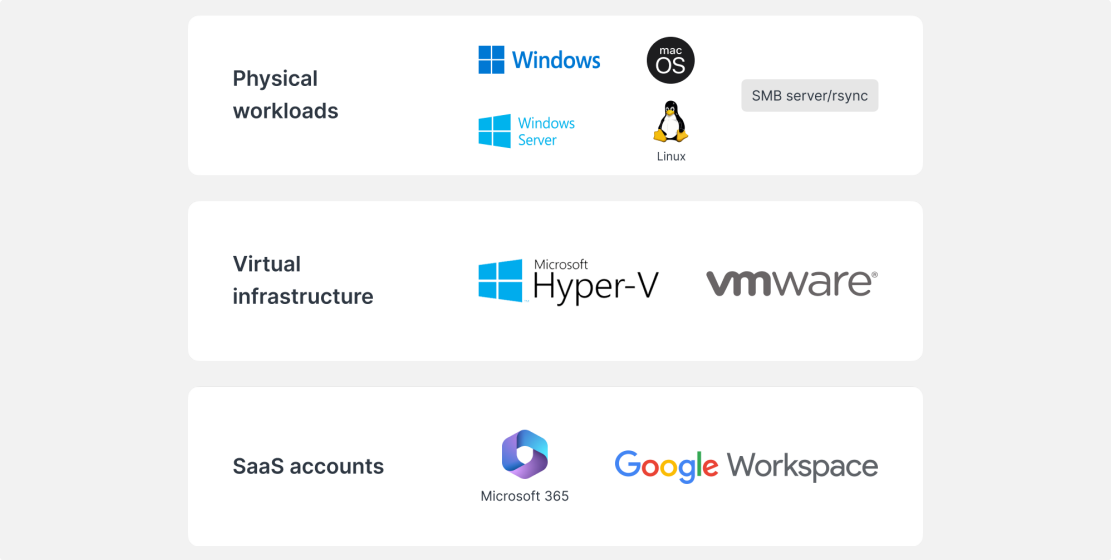
Beskyt slutpunkter i tilfælde af ondsindede angreb med effektiv backup fra bunden og fleksibel gendannelse på filniveau.

Virtuel infrastruktur

Tag backup af VMware® vSphere™, Microsoft® Hyper-V® VM'er og LUN'er med effektive teknologier til datareduktion.

SaaS-konti

Aktivér kontinuerlig beskyttelse af data, der er gemt i skyen, med automatisk registrering af nyligt tilføjede konti.



Effektiv genoprettelse

Minimer nedetid for kritiske produktionssystemer ved hurtigt at gendanne backupkopier fra et lokalt eller eksternt Synology-system.

Næsten nul RTO

Monter backupbilleder på VMware®, Hyper-V® eller Synology Virtual Machine Manager for at genoptage arbejdet så hurtigt som muligt. Gendan VM'er til en alternativ hypervisor for at undgå driftsforstyrrelser.

Minimal RPO

Konfigurer backupfrekvensen i henhold til dine behov, og minimer mængden af data, der potentielt kan blive påvirket under et angreb. Beskyt systemer hurtigt takket være trinvis backup og deduplikeringsteknologi.

Intuitiv betjening

Lad medarbejderne gennemse og se e-mails, kontakter og filer fra en praktisk portal, før de gendannes, så de får en mere brugervenlig oplevelse og reducerer byrden for IT-medarbejdere.

Tilføj et ekstra sikkerhedslag

Overhold 3-2-1-strategien for backup ved at gemme et tredje sæt data eksternt eller i skyen, så dine data beskyttes mod brand, naturkatastrofer eller tyveri.

Til eksterne servere

Gem backupkopier på en Synology-server på en sekundær placering for at beskytte mod fysiske katastrofer, og kopier uforanderlige snapshots for ekstra beskyttelse mod ransomware.

Til skyen

Tag backup til en hvilken som helst større udbyder af skylager, og sørg for, at dine data er beskyttet mod uautoriseret adgang via AES-256-kryptering på klientsiden. https://c2.synology.com/storage/nas

Anvendes på tværs af brancher

"Synology [...] giver os mulighed for at reducere udgifterne til serverhardware [...], samtidig med at backup af infrastruktur og arbejdsstationer, systemlogning og filstyring bliver meget nemmere."
https://www.synology.com/company/case_study/Investortools

"Takket være Active Backup for Business er alle vores backups nu centraliseret og tilgængelige døgnet rundt, hvilket hjælper os med at minimere nedetid og overholde FERPA's regler."
https://www.synology.com/company/case_study/University_of_Washington

"[...] Active Backup for Business har utrolige backuphastigheder og udfører også mirakler utrolig ved sletning af dublerede data - det optog kun 28 TB ud af de samlede 58 TB på serveren. [...]"
https://www.synology.com/company/case_study/SHISEIDO_Taiwan_ABB

"[...] Active Backup for Business [...] giver os mulighed for at centralisere og administrere alle backupopgaver fra en enkelt konsol. Hurtig og pålidelig genoprettelse sikrer også forretningskontinuitet."
https://www.synology.com/company/case_study/UNESCO

Ofte stillede spørgsmål

Hvad er ransomware?

Ransomware er en type malware, der krypterer ofrenes filer. Hackerne, der kræver løsepenge for at genoprette dataadgangen, truer ofte med permanent at ødelægge data, hvis der ikke betales løsepenge. Ransomware-angreb kan være meget forstyrrende og kan forårsage betydelige økonomiske tab for enkeltpersoner og organisationer. Det er vigtigt at beskytte dig selv og dine enheder mod ransomware, f.eks. ved at holde din software opdateret og regelmæssigt tage backup af dine filer.

Hvilke typer ransomware findes der?

Der er mange forskellige typer ransomware, og der udvikles konstant nye versioner. Nogle af de mest almindelige typer ransomware omfatter:

- **Kryptering med ransomware** - Den mest almindelige type ransomware krypterer offerets filer, så de ikke kan åbnes uden dekrypteringsnøglen. Hackere kræver derefter løsepenge som betaling for nøglen
- **Låsende ransomware** - En type ransomware, der låser ofre ude af deres computer ved at ændre login-legitimationsoplysninger eller vise en meddelelse, der forhindrer offeret i at få adgang til deres system. Hackere kræver derefter løsepenge som betaling for at låse op for computeren
- **Ransomware-as-a-Service (RaaS)** - En forretningsmodel, hvor hackere tilbyder ransomware til andre personer eller grupper, der ønsker at udføre angreb. Førstnævnte vil typisk levere ransomware og håndtere betalinger, mens sidstnævnte modtager en procentdel af løsesumsbetalingerne
- **Scareware** - Ransomware, der er designet til at skræmme ofre til at betale løsepenge. Det drejer sig typisk om at vise falske sikkerhedsadvarsler eller meddelelser, der hævder, at offerets computer er inficeret med en virus. Hackeren vil derefter kræve løsepenge for at fjerne den formodede infektion

Hvordan spreder ransomware sig?

Ransomware spredes typisk via phishing-e-mails eller ved at udnytte sårbarheder i et computersystem. I et phishing-angreb sender en hacker en e-mail, der ser ud til at være fra en legitim kilde, f.eks. en bank eller en velkendt virksomhed. E-mailen vil ofte indeholde et link eller en vedhæftet fil, der, når der klikkes på den, installerer ransomware på offerets computer. Udnyttelse af sårbarheder i et system foregår på lignende måde, bortset fra at hackeren vil bruge en fejl i systemets sikkerhed til at installere ransomware uden offerets viden. I begge tilfælde, når ransomware er installeret, kan det hurtigt sprede sig til andre computere på samme netværk.

Hvad er den typiske proces i et ransomware-angreb?

Processen med et ransomware-angreb følger typisk disse trin:

1. Hackeren får adgang til et offers computer enten ved at sende en phishing-e-mail eller ved at udnytte en sårbarhed i systemet
2. Når hackeren har adgang til offerets computer, vil vedkommende installere ransomware på systemet
3. Ransomwaren vil derefter kryptere offerets filer, hvilket gør dem utilgængelige for brugeren
4. Hackeren vil så kræve løsepenge fra offeret, typisk i form af en digital valuta som Bitcoin, for den dekrypteringsnøgle, der låser de krypterede filer op
5. Hvis offeret betaler løsepenge, vil hackeren levere dekrypteringsnøglen, og offeret vil kunne få adgang til sine filer igen. Der er dog ingen garanti for, at hackeren rent faktisk leverer nøglen, og selv om vedkommende gør det, kan offerets filer blive beskadiget eller ødelagt som følge af krypteringsprocessen

Det er vigtigt at bemærke, at der er mange variationer i denne proces, og ikke alle ransomware-angreb vil præcist følge disse trin. Nogle angreb involverer muligvis slet ikke kryptering af filer, mens andre kan omfatte andre former for afpresning.

Hvordan kan jeg få ransomware?

Du kan få ransomware på flere måder. En af de mest almindelige måder er ved at klikke på et ondsindet link eller en vedhæftet fil i en phishing-e-mail. Denne type e-mail er designet til at se legitim ud, og det ser ofte ud til at være fra en velkendt virksomhed eller organisation. Når du klikker på linket eller den vedhæftede fil, installeres ransomwaren på din computer. En anden måde, du kan få ransomware på, er ved at besøge et inficeret websted. Disse websteder er blevet hacket af hackere, som har indsat en kode, der automatisk installerer ransomware på din computer, hvis du besøger webstedet. Du kan også få ransomware ved at downloade inficerede filer fra internettet. Dette kan ske, hvis du downloader en fil fra et mistænkeligt websted, eller hvis du downloader en fil, der er blevet delt af en person, du ikke kender. Kort sagt er det vigtigt at være forsigtig, når du surfer på internettet, og at undgå at klikke på links eller downloade filer fra ukendte kilder. Dette kan hjælpe med at beskytte dig mod at få ransomware og andre typer malware.

Hvem er mål for ransomware?

Ransomware-angreb kan være rettet mod alle, der bruger en computer eller en anden enhed, der er forbundet til internettet. Nogle grupper er dog mere tilbøjelige til at blive angrebet end andre. For eksempel er ransomware-angreb ofte rettet mod virksomheder, da de ofte har mere værdifulde data og kan være mere villige til at betale løsepenge for at få adgang til dem igen. Hospitaler, skoler og andre organisationer, der leverer vigtige tjenester, er også almindelige mål, da et ransomware-angreb kan forstyrre deres aktiviteter og bringe folks liv i fare. Enkeltpersoner kan også være mål for ransomware-angreb. I disse tilfælde kan hackerne forsøge at afpresse offeret for penge ved at true med at slette deres personlige filer eller offentliggøre følsomme oplysninger, medmindre der betales løsepenge. Målene for ransomware-angreb vælges ofte baseret på værdien af deres data og deres villighed til at betale løsepenge for at få dem tilbage.

Hvad er risiciene ved at betale ransomware?

At betale en løsepenge til en ransomware-hacker kan synes at være den nemmeste måde at få sine filer tilbage på, men det kan faktisk være en meget risikabel beslutning. Der er flere risici forbundet med at betale løsepenge, herunder:

- Der er ingen garanti for, at hackeren faktisk leverer dekrypteringsnøglen. I mange tilfælde modtager ofre, der betaler løsepenge, aldrig nøglen og er ude af stand til at få adgang til deres filer
- Betaling af løsepenge kan måske opmuntre hackere til at fortsætte deres angreb. Hvis hackerne ved, at ofrene er villige til at betale løsepenge, kan de være mere tilbøjelige til at udføre flere angreb i fremtiden
- Betaling af løsepenge kan gøre dig til et mål for fremtidige angreb. Hvis hackeren ved, at du er villig til at betale en løsesum, vil du muligvis være mere tilbøjelig til at blive angrebet i fremtiden
- Betaling af løsepenge kan være ulovligt. I nogle tilfælde kan betaling af løsepenge til en kriminel organisation betragtes som en form for finansiering af terrorisme eller andre ulovlige aktiviteter

Selv om betaling af løsepenge kan virke som den nemmeste måde at få adgang til dine filer på, kan det faktisk være en meget risikabel beslutning. Det er vigtigt nøje at overveje risiciene, før der træffes en beslutning.

Hvad er omkostningen ved ransomware?

Omkostningerne ved et ransomware-angreb kan variere meget afhængigt af en række faktorer, f.eks. den anvendte type ransomware, antallet af krypterede filer og effektiviteten af angrebet. I nogle tilfælde kan omkostningerne ved et ransomware-angreb være relativt lave, hvis hackerne kræver et par hundrede dollars i løsepenge. I andre tilfælde kan omkostningerne være meget højere, hvis hackere kræver tusindvis af dollars eller endnu mere for at genoprette adgangen til offerets filer. Ud over de direkte omkostninger i forbindelse med betaling af løsepenge kan ransomware-angreb også have betydelige indirekte omkostninger. Et ransomware-angreb kan f.eks. forårsage nedetid og tab af produktivitet, hvilket kan resultere i tabt omsætning og indtjening. Det kan også skade en virksomheds omdømme og kundernes tillid, hvilket kan have langsigtede negative konsekvenser for virksomheden. Disse indirekte omkostninger er ofte meget højere end selve løsepengene.

Hvad er symptomerne ved ransomware?

Symptomerne på et ransomware-angreb kan variere afhængigt af den specifikke type ransomware, der anvendes. Nogle almindelige symptomer omfatter:

- Dine filer er krypterede, og du kan ikke få adgang til dem
- Du modtager en meddelelse fra en hacker, der kræver en løsesum til gengæld for en dekrypteringsnøgle
- Du ser ukendte programmer eller processer, der kører på din computer
- Computeren bliver langsom eller reagerer ikke
- computeren viser usædvanlige fejlmeddelelser eller pop-up-vinduer

Hvis du har mistanke om, at din computer er blevet inficeret med ransomware, er det vigtigt at reagere hurtigt. Frakobl din computer fra internettet for at forhindre, at ransomwaren spreder sig.

Hvordan forhindres ransomware-angreb?

Du kan tage flere forholdsregler for at forhindre et angreb, herunder:

- Brug velrenommeret antivirus- eller sikkerhedssoftware, og hold det opdateret. Dette kan være med til at beskytte din computer mod ransomware og andre typer malware
- Vær forsigtig, når du åbner vedhæftede filer eller links i mails. Ransomware leveres ofte via phishing-mails, så det er vigtigt at være opmærksom på, hvad du klikker på
- Sørg for at holde operativsystemet og anden software opdateret. Softwareopdateringer omfatter ofte sikkerhedsrettelser, der kan hjælpe med at beskytte computeren mod ransomware og andre trusler
- Tag regelmæssigt backup. Dette kan hjælpe med at beskytte dine data, hvis din computer er inficeret med ransomware. Sørg for at overholde en af de anbefalede backupstrategier, f.eks. 3-2-1-strategien for backup
- Vær opmærksom på risiciene ved ransomware, og oplær andre i din organisation om disse trusler. Dette kan hjælpe med at forhindre ransomware-angreb og gøre det nemmere at registrere og reagere på dem, hvis de opstår

Den bedste måde at forhindre ransomware-angreb på er at være på vagt og holde din computer og dine data beskyttet. Dette kan medvirke til at reducere risikoen for et ransomware-angreb og gøre det nemmere at komme sig efter et, hvis det sker.

Hvordan kan Synology beskytte mig mod ransomware?

Forebyggende handlinger er afgørende for at undgå at blive offer for ransomware. Brug disse Synology-løsninger som supplement til din foretrukne antivirussoftware:

- **Forhindr adgang** - Reducer spredningen af ransomware ved at angive tilladelser for filer, programmer og adgang, og konfigurer sikre loginoplysninger ved hjælp af Secure SignIn og C2 Password
  .
- **Beskyt enheder** - Forældede systemer er i større fare. Opdater alle dine NAS på én gang med Synology Central Management System (CMS), og beskyt andre enheder ved hjælp af gruppepolitikker i Synology Directory Server og C2 Identity
- **Undgå mistænkelige filer** - Spam og phishing-e-mails, der indeholder mistænkelige filer, er almindelige metoder til at sprede ransomware. Synology MailPlus leverer effektiv beskyttelse mod malware og forebygger spam
- **Kontrollér, om der er sårbarheder** - Brug Synology Security Advisor til rutinemæssigt at søge efter malware, sårbarheder og unormale loginaktiviteter. Implementer anbefalede ændringer for at forbedre NAS-sikkerheden.
  https://www.synology.com/dsm/overview/security

Flere måder at beskytte dine data på

Administration af din flåde

Benyt de omfattende funktioner til at administrere dataadgangstilladelser, softwarestatus, systemtilstand og meget mere centralt.
https://www.synology.com/dsm/overview/administration

Overvåg alle dine systemer

Identificer mistænkelige loginaktiviteter, administrer opdateringer og overvåg enhedens tilstand, uanset hvor dine enheder er placeret.
https://www.synology.com/dsm/feature/active-insight

Beskyt dine data

Følg 3-2-1-reglen for backup for at beskytte dine data mod utilsigtede og ondsindede ændringer eller sletning.
https://www.synology.com/dsm/solution/data_backup

Kom i gang

Kontakt os

Kontakt regionale salgsafdelinger for at få yderligere oplysninger
https://www.synology.com/form/inquiry/sales

Hvor kan du købe den

Find en Synology-partner i dit område
https://www.synology.com/wheretobuy

Notes:

1. eSentire, 2022 Official Cybercrime Report
   https://www.esentire.com/resources/library/2022-official-cybercrime-report

Beskyt din organisation mod ransomware

https://www.synology.com/da-dk/dsm/solution/ransomware

Synology hjemmeside

https://www.synology.com/

Kontakt os

https://www.synology.com/company/contact_us