CrowdStrike nedbrud

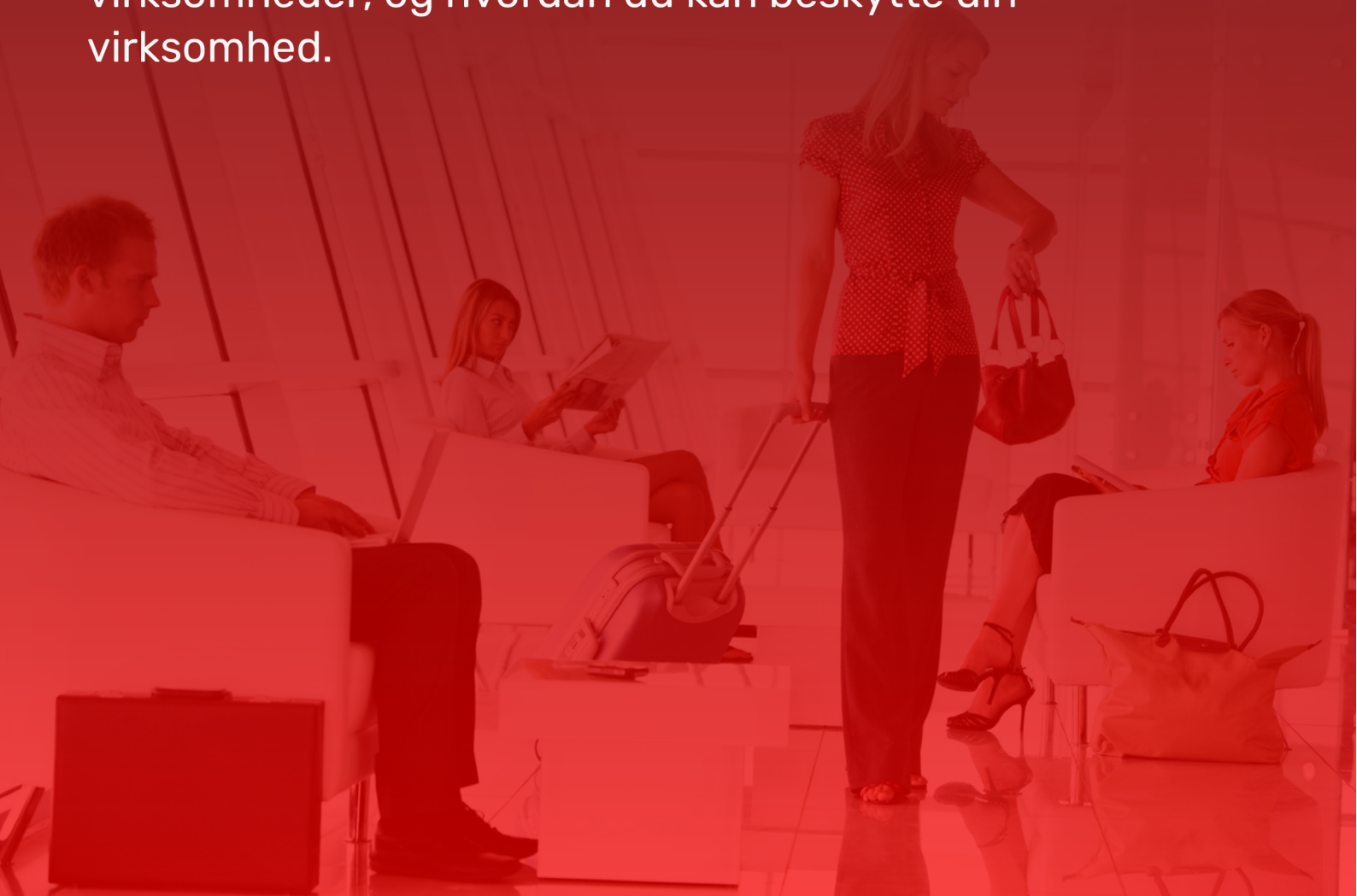
Forstå CrowdStrike-nedbruddet

novaram INTEGRITY

Den 19. juli 2024 medførte en rutinemæssig softwareopdatering fra CrowdStrike et stort problem, der påvirkede omtrent 8½ millioner Windows-computere.

Denne hændelse forårsagede betydelige forstyrrelser i mange brancher, herunder lufthavne, supermarkeder og medier.

Her forklarer vi hvad CrowdStrike er, hvad der gik galt med opdateringen, hvordan det påvirkede virksomheder, og hvordan du kan beskytte din virksomhed.



Hvad er CrowdStrike?

CrowdStrike er en førende virksomhed inden for cybersikkerhed, grundlagt i 2011 og baseret i USA. I bund og grund fungerer de som digitale livvagter for virksomheder og store organisationer, hvor de beskytter dem mod cybertrusler som ransomware, malware og andre online angreb.

CrowdStrike er betroet af et bredt spektrum af virksomheder, herunder mere end 500 virksomheder fra Fortune 1000-listen. De har et solidt ry for hurtigt at reagere på cybersikkerhedstrusler og har været involveret i undersøgelsen af større cyberhændelser. Deres hovedprodukt hedder Falcon-sensor. Dette skybaserede sikkerhedssystem er designet til at opdage og stoppe cybertrusler i realtid.

Hvad er Falcon sensor?

Forestil dig, at din computer er et hus. Regelmæssig antivirussoftware er som et sikkerhedssystem, der leder efter specifikke typer af "skurke" (som indbrudstyve), som det genkender fra tidligere. Hvis det ser nogen af disse kendte skurke, forhindrer det dem i at komme ind.

Falcon-sensor er noget mere, kendt som et EDR (Endpoint Detection and Response). Det er som at have en intelligent sikkerhedsvagt for dit hus. Denne vagt kigger ikke kun efter de skurke, som antivirusprogrammet kender, men holder også øje med enhver mærkelig eller mistænkelig aktivitet. Vagten kan også undersøge ukendte situationer og træffe foranstaltninger for at beskytte dit hus, selvom truslen er noget nyt.

Så mens et antivirusprogram er godt til at stoppe kendte trusler, er et EDR meget bedre til at håndtere nye og uventede trusler for at holde din computer sikker. Ulempen er, at EDR kræver et dybere adgangsniveau.

EDR kræver hurtige opdateringer for at holde trit med hurtigt skiftende trusler. I modsætning til andre softwareopdateringer kan disse ikke udrulles i faser..

Hvad skete der?

Den 19. juli forårsagede en rutinemæssig softwareopdatering fra CrowdStrike store forstyrrelser for mange virksomheder over hele verden.

Tidligt om morgenen frigav CrowdStrike en opdatering til deres program Falcon-sensor. Denne opdatering var beregnet til at forbedre sikkerheden ved at målrette specifikke værktøjer, der anvendes i cyberangreb. Men opdateringen indeholdt en kodningsfejl, kendt som en "logisk fejl."

Denne fejl forårsagede, at Windows-computere, der kørte Falcon-sensor, brød sammen, hvilket førte til den berygtede "Blue Screen of Death" (BSOD).

Virkningen var øjeblikkelig og udbredt.

Mange virksomheder fandt deres Windows-computere ubrugelige, hvilket resulterede i betydelige forstyrrelser. Lufthavne oplevede kaos, da deres systemer svigtede, supermarkedskasser fungerede ikke, og journalister havde vanskeligheder med at rapportere om problemet på grund af deres nedbrudte udstyr.

Problemet påvirkede millioner af enheder globalt. Folk rapporterede, at deres computere gik ind i en genstartsløkke, hvilket gjorde det umuligt at bruge dem.

CrowdStrike reagerede hurtigt. Inden for en time efter identifikationen af problemet begyndte de at arbejde på en løsning. Klokken 7:27 dansk tid, frigav de en opdatering for at rette de fejlagtige konfigurationsfiler.

Men genopretnings-processen varierede. For mange kunne problemet løses fjernstyret ved at slette den problematiske fil, hvis systemet var online. For dem med offline systemer var manuel sletning af filen nødvendig, hvilket ofte krævede hjælp fra IT-support.

Hvad var konsekvenserne for virksomheder ?

CrowdStrike-nedbruddet havde enorme konsekvenser for virksomheder på tværs af mange brancher.

Lufthavne og flyselskaber

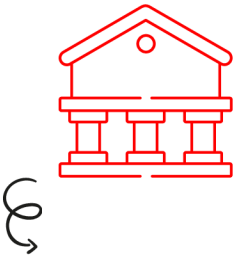
Nedbruddet førte til betydelige forstyrrelser på lufthavne. Systemer, der håndterer flyplaner, billetsalg og kundeservice blev ramt, hvilket forårsagede forsinkelser og forvirring. Passagerer oplevede lange køer og forsinkelser, da lufthavnspersonalet kæmpede med at håndtere uden deres sædvanlige digitale værktøjer.

Supermarkeder og detailhandel

Mange supermarkedskasser fungerede ikke, hvilket gjorde det umuligt at behandle salg. Dette førte til frustrerede kunder og tabte salg, da butikkerne kæmpede for at fungere uden deres point-of-sale-systemer. Nogle detailhandlere måtte lukke midlertidigt, indtil deres systemer blev genoprettet..

Medier og journalistik

Journalister og medievirksomheder stod over for store udfordringer, da deres computere brød sammen, hvilket efterlod dem uden de væsentlige værktøjer, der var nødvendige for at rapportere om hændelsen. Dette forstyrrede nyhedsdækningen og evnen til at levere rettidige opdateringer til offentligheden.



Banker og finansielle tjenester

Den finansielle sektor mærkede også virkningerne, da banker oplevede systemnedbrud, der påvirkede transaktioner og kundeservice. Online banktjenester blev forstyrret, hvilket førte til vanskeligheder for kunder, der forsøgte at få adgang til deres konti eller udføre finansielle transaktioner.

Generelle forretninger

På tværs af brancher oplevede virksomheder, der var afhængige af Windows-systemer, produktivitetstab. Ansatte kunne ikke få adgang til vigtige filer, kommunikere effektivt eller udføre deres sædvanlige opgaver. Mange virksomheder fandt det vanskeligt at yde kundesupport, da deres systemer var nede. Callcentre og online helpdesks oplevede øgede mængder af forespørgsler og klager, hvilket yderligere belastede ressourcerne.

Sundhedsvæsenet

Selvom det ikke blev så bredt rapporteret, kunne sundhedsinstitutioner, der anvendte berørte systemer, have oplevet forsinkelser i adgangen til patientjournaler, planlægning og andre kritiske operationer, hvilket potentielt kunne påvirke patientplejen.

Samlet set demonstrerede CrowdStrike-nedbruddet, hvor afgørende pålidelige cybersikkerhedsværktøjer er for forretningskontinuitet. Det fremhævede, hvor sammenkoblede moderne forretningsoperationer er, og den udbredte indvirkning, som et enkelt softwareproblem kan have.

> Virksomheder vil sandsynligvis nu gennemgå deres beredskabsplaner og IT-supportberedskab for bedre at kunne håndtere lignende hændelser i fremtiden.

Hvordan vi kan hjælpe din virksomhed

Mange virksomheder gennemgår nu deres katastrofeberedskabsplaner og forretningskontinuitetssoftware. De ønsker at sikre sig, at de har klare procedurer for at hjælpe med at mildne virkningerne af fremtidige forstyrrelser.

Hos Novaram hjælper vi virksomheder med at holde sig sikre fra cybertrusler samtidig med at deres teams forbliver produktive. Det gør vi gennem god IT-planlægning og support.

Lad os om at gennemgå jeres nuværende IT og/eller planlægge en strategi for at sikre, at jeres virksomhed er beskyttet.

Kontakt os

RING: 70267730
EMAIL: info@novaram.dk
WEBSITE: novaram.dk

novaram
INTEGRITY