Dansk hostingselskab lagt ned af ransomware: Kunder har mistet al data

PLUS It-sikkerhed 22. august kl. 17:00 24

Claus Pilgaard, der står bag virksomheden Chili Klaus, var en af dem, der mærkede konsekvenserne, da hostingselskabet Azerocloud fredag blev ramt af et ransomware-angreb. Illustration: Kåre Viemose/BAM/Ritzau Scanpix.

Det danske hostingselskab Azerocloud er »lammet fuldstændig« efter at være blevet ramt af et ransomware-angreb. Selskabet opfordrer kunder til at flytte over til andre firmaer.

Christoffer Elmann Ranhauge
Journalist

Artiklen er ældre end 30 dage

Artiklen er ældre end 30 dage

Det danske hostingselskab Azerocloud er blevet ramt af et ransomware-rangreb, der siden natten til fredag har skabt store problemer for både firmaet og dets kunder.

Angrebet har ramt centrale dele af hostingselskabets funktioner. Det gælder både hjemmesider, email-systemer, kundesystemer og kundernes hjemmesider.

Kort sagt »alt,« som Azerocloud selv oplyser på selskabets hjemmeside.

Virksomheden har ikke kunnet genskabe data, og dermed har størstedelen af selskabets kunder ifølge Azerocloud selv »mistet alt data hos os«.

»Vi er dybt berørte over situationen, og er klar over, at angrebet også er meget kritisk for mange af vores kunder. Udover data, mistede vi også alle vores systemer og servere og har haft svært ved at kommunikere,« lyder det i en besked til selskabets kunder.

Flere hundrede kunder ramt

Azerocloud og dets underselskab Cloudnordic, som også blev ramt af angrebet, har ifølge selskaberne selv mellem 200 og 300 kunder, der både tæller helt små virksomheder og mellemstore firmaer.

Blandt kunderne var flere selvstændige erhvervsdrivende, webshops og foreninger landet over, og de har også mærket konsekvenserne af angrebet mod Azerocloud.

En af dem, der har mærket konsekvenserne ved angrebet og nedbruddet, er internetfænomenet Chili Klaus. Da han om fredagen tjekkede sin mail, virkede den ikke. Samtidig eksisterede

den hjemmeside, hvor han normalt sælger både hot sauces og stærke chokolader, pludselig heller ikke.

»Da det stod klart for mig, at vi havde mistet vores data, fik jeg helt ondt i maven. Det får jeg også, når vi taler om det nu. Det kommer til at koste os kassen, og det har det jo allerede gjort, for vi har været væk fra world wide web i fem dage, og det duer jo ikke, når man har butik,« siger Chili Klaus, som bærer det borgerlige navn Claus Pilgaard til Version2.

Kan ikke genskabe data

Ifølge Azeroclouds egne undersøgelser startede angrebet natten til fredag, hvor samtlige af virksomhedens systemer blev ramt.

Hackerne fik tilsyneladende adgang til systemerne i forbindelse med, at selskabets servere skulle flyttes fra et datacenter til et andet.

»Under arbejdet med at flytte servere fra det ene datacenter til det andet datacenter, blev servere, der tidligere var på separate netværk, beklageligvis kablet sådan at de fik adgang til vores interne netværk, der bruges til administration af alle vores servere,« skriver Azerocloud.

Dette var kritisk, fordi nogle af serverne inden flytningen var blevet inficeret af malware. Det var sket, uden at man fra Azeroclouds side havde opdaget det, oplyser selskabet på sin hjemmeside.

»Via det interne netværk, fik angriberne adgang til helt centrale administrationssystemer og backupsystemerne,« skriver selskabet, som samtidig oplyser, at al data og alle backupsystemer blev ramt.

»Det lykkedes angriberne at lave en kryptering af alle serveres diske, samt på primært og sekundært backupsystem, hvorved alle maskiner gik ned, og vi mistede adgang til alt data.«

Kriminelle går efter hostingudbydere

Angrebet mod Azerocloud skriver sig ind i en længere række af angreb mod hostingudbydere. Sådan lyder det fra Jacob Herbst, der er CTO i it-sikkerhedsvirksomheden Dubex og medlem af Cybersikkerhedsrådet.

»Set fra de kriminelles side er hostingudbydere rigtig interessante, fordi de også vil være i en klemme i forhold til deres kunder. Der er en masse erhvervsdrivende, som har tillid til deres leverandør, og når leverandøren så bliver ramt, kan det ramme rigtig bredt og i flere led,« siger Jacob Herbst.

I Azeroclouds tilfælde tyder det ifølge Jacob Herbst på, at hostingselskabet backup-løsning ikke har været tilstrækkeligt beskyttet og afkoblet fra driftsmiljøet.

»De kriminelle går målrettet efter backuppen, da det ofte er det eneste som står mellem dem og mulig betaling af løsepenge. Derfor er ekstra beskyttelse af backuppen i dag et krav, og backuppen bør som minimum være adskilt fra den øvrige infrastruktur,« siger Jacob Herbst.

'Vi er rasende kede af det'

Hos Azerocloud ser direktør Martin Haslund Johansson med stor alvor på sagen.

Han oplyser, at selskabet er blevet mødt med et krav fra gerningspersonerne om at betale en løsesum på seks bitcoins for at få data låst op igen. Det har virksomheden afvist, og sagen er i stedet meldt til politiet, forklarer direktøren.

»De foreløbige undersøgelser peger på, at angriberne er kommet ind via Microsoft eller VMWare,« siger han.

Sårbarheder i software fra VMware er førhen blevet udnyttet i både USA og Europa, og tidligere i år advarede Center for Cybersikkerhed om, at sårbarheden stadig blev udnyttet til at installere ransomware.

Har I sikret jer godt nok, når sådan noget kan ske?

SPONSERET INDHOLD

Version2 Briefing i Aarhus: Beskyttelse af kritisk infrastruktur og OT

IoT

»Hvis vi havde opdelt vores systemer bedre, så havde vi jo gjort det godt nok. Vi kunne åbenlyst have gjort det bedre, men vi har gjort det bedste vi kunne med det, vi har haft,« siger Martin Haslund Johansson.

»Man kan altid slå sig selv oven i hovedet med, om man skulle have gjort noget anderledes, og det kommer jeg nok til at gøre de næste mange år. Vi er rasende kede af, hvordan det her har spillet sig ud for vores kunder«.

Flere af kunderne har blandt andet givet udtryk for frustrationer over, at de ikke hurtigere har fået hurtigere information om, hvad der er sket. De følelser har direktøren forståelse for, forklarer han.

»Vi er tre ansatte, og vi har haft så få hænder til at lave det her med. Vi har haft statussider, og selvfølgelig kunne de have været opdateret hurtigere og oftere, men vi havde de hænder, vi havde. Jeg kan godt forstå frustrationen, men jeg har også fået en hel anden respekt for de store virksomheder, når de kommer i den her slags situationer,« siger Martin Haslund Johansson.

BRIEFING | Digitale Integratorer: Tiltrækning og udvikling af tidens mest efterspurgte medarbejdergruppe

Han peger samtidig på, at angrebet meget vel kan blive dødsstødet for virksomheden.

»Hvis man har kunder, så har man en virksomhed, og jeg forventer ikke, at vi har kunder efter det her. Vi gør alt, hvad vi kan for at hjælpe kunderne til en produktiv tilstand. Og når støvet er faldet, må vi se, hvad der så er tilbage,« siger han.

Hundredvis af firmaer skulle pludselig skifte navneserver: Ransomware gav stormløb på domæneudbyder

Chili Klaus og 300 andre firmaer gik i sort efter angreb på dansk netudbyder: »Det kommer til at koste kassen«

Denne artikel

Mærsk-selskab ramt af ransomware: »Vi er er ved at undersøge sagen nærmere«

It-sikkerhedsekspert: Hackerangreb mod 7/11 »virker ret standard«

Dansk undertøjsgigant klædt af: JBS ramt af dobbelt afpresningsangreb

Ransomware-kriminelle kræver løsesum af nordens største hotelkæde: »Kommer ikke til at ske«

Fokus

V2 Security

Emner

It-sikkerhed | Hacking | Ransomware