Var tæt på at slukke tusindvis af vindmøller: Nu fortæller Vestas om cyberangreb

dr.dk/nyheder/viden/teknologi/frygtede-skulle-lukke-alle-vindmoeller-nu-aabner-vestas-op-om-hacking-angreb

Allan Nisgaard February 14, 2022

Fredag den 19. november 2021 klokken otte om aftenen får topchef i Vestas, Henrik Andersen, sved på panden.

Vindmøllegiganten, der har 80.000 vindmøller fordelt på hele kloden, er nemlig blevet ramt af et såkaldt ransomware-angreb.

Cyberkriminelle er trængt dybt ind i Vestas' netværk og har sat en væsentlig del af systemerne ud af funktion. For at åbne dem igen kræver de løsepenge.

Det er uklart, om hackerne også har skaffet sig adgang til de systemer, der styrer vindmøllerne. Det skal Henrik Andersen og hans hold finde ud af - og det skal gå stærkt.

Hvis Vestas af forsigtighed trykker på den helt store knap og slukker for de 50.000 vindmøller, de selv har direkte adgang til, kan millioner af borgere stå uden strøm.

> Russiske hackere - både dem, der går efter penge, og de statsstøttede - har samme motiv. De vil finde et stort mål, hvor de kan lave så meget kaos som muligt.
> *Andy Greenberg, journalist på Wired magazin og forfatter til bogen Sandworm.*

Lukker Vestas ned, risikerer de, at hackerne kan udrette skader på vindmøllerne, som kan tage måneder at fikse.

- Alt er i princippet kritisk, indtil man når til et stadie, hvor man kender fakta, siger Henrik Andersen.

For første gang siden hackerangrebet åbner Vestas nu op og går i detaljer om hændelsen, der har påvirket topchefen kraftigt.

- Det er noget, der for altid sætter sig dybt i éns person, siger Henrik Andersen.

Hvem hackede Vestas?

Ransomware-angrebet mod Vestas blev udført med en type af ransomware, som hedder Lockbit 2.0. Gruppen bag Lockbit har rødder i Rusland og har angrebet blandt andet hospitaler og energiselskaber i en række lande.

Lockbit opererer efter en såkaldt affiliate model, hvor godkendte "partnere" gennemfører selve angrebet og afpresningen, mens gruppen bag tager sig af det tekniske og indkasserer en procentdel af ofrenes betalinger.

Blandt andet blev det italienske energiselskab ERG ramt af Lockbit 2.0., og herhjemme angreb hackere Kalundborg Forsyning med samme ransomware. Kalundborg Forsyning valgte dog ikke at betale nogen løsesum.

Truslen mod energisektoren er ’meget høj’

Når en vindmøllegigant som Vestas bliver angrebet af hackere, kan det i værste tilfælde få langt større konsekvenser end låste systemer og tabte millionbeløb.

Vestas er nemlig det, vi kalder kritisk infrastruktur.

Alt det, vi betragter som samfundskritisk – heriblandt telekommunikation, veje, vandforsyning, skibstrafik, hospitalsvæsnet og elektricitet - er i dag forbundet elektronisk og derfor sårbart overfor cyberangreb.

- Ude i verden tænker man på Danmark som landet bag Mærsk, Lego og Vestas. To ud af de tre (Mærsk og Vestas, red.) har allerede været ramt af cyberangreb. Så det sker allerede, siger Andy Greenberg, der er journalist på Wired Magazine og forfatter til bogen Sandworm, der i cyber-kredse er en slags bibel.

Bogen beskriver, hvordan Kremls berygtede cyberenhed, Sandworm, lammede Mærsks globale operationer, fordi den danske shipping-gigant ved et tilfælde blev trukket ind i Ruslands cyberkrig mod Ukraine.

- I den her nye virkelighed med cyberanbreb er fysisk afstand ikke noget forsvar. Et land som Danmark har faktisk fjenderne stående lige foran hoveddøren, fortsætter Andy Greenberg.

Vestas' turbiner kan levere strøm til 240 millioner europæeres årlige energiforbrug, hvilket er over halvdelen af EU's befolkning. De er dermed en vigtig del af energisektoren.

> Jeg er meget bekymret og følsom over, at nogle af vores medarbejdere ser dem selv blive taget med i sådan en konflikt her.
> *Henrik Andersen, CEO topchef i Vestas*

Og den sektor er sårbar overfor cyberangreb, forklarer Søren Maigaard, der er direktør hos energisektorens cybersikkerhedsenhed, EnergiCERT.

- Worst case-scenariet er, at nogle får kontrol over den kritiske infrastruktur og lukker ned for eksempelvis varmen eller for strømmen i et mindre område. Det skal understreges, at det er ekstraordinært svært at gøre. Men derfor skal man stadig passe på, fortsætter Søren Maigaard, der ikke ønsker at forholde sig til angrebet mod Vestas.

Truslen fra ransomware-angreb mod den danske energisektor er vurderet til at være 'meget høj' af Center for Cybersikkerhed.

Det er den blandt andet vurderet til at være, efter USA sidste år oplevede det største cyberangreb mod deres energi-infrastruktur nogensinde.

Cyberkriminelle fik ram på landets største rørledning, Colonial Pipeline, der hver dag transporterer 378 millioner liter olie på den amerikanske østkyst.

Da Colonial Pipeline ikke vidste, hvor seriøst det stod til, og heller ikke var i stand til at fakturere for olien, valgte de helt at lukke rørledningen i seks dage. Det på trods af at Colonial dagen efter angrebet betalte angriberne 5 millioner dollars for at få systemerne låst op igen.

Både den amerikanske regering og FBI blev involveret i situationen, der risikerede at hæve amerikanske benzinpriser markant.

- Når jeg kigger tilbage på det, så er det en lærerig erfaring. Men det er nok en af de dyrere købte erfaringer, lyder det fra topchef i Vestas Henrik Andersen. (© DR)

Truer med at offentliggøre stjålne dokumenter

Da Vestas får bekræftet, at der er tale om et cyberangreb, går de næste timer med at opklare præcis, hvor seriøst det står til.

- Fra det tidspunkt tager vi det simpelthen en time ad gangen, siger Henrik Andersen.

Klokken tre om natten står det klart, at hackerne ikke har formået at trænge ind til de systemer, der styrer Vestas' mange møller rundt i verden.

- Det gør, at vi kan træffe beslutningen om ikke at lukke for vores turbiner i hele verden. Men vi lukker stort set alt andet ned, siger Henrik Andersen og fortsætter:

- Hele vores kommunikationsdel kan dog fortsætte upåvirket. Så vores mail, vores teams og vores videoer kan køre videre. Det er en stor fordel.

Hackerangrebet er dog langt fra overstået for Vestas, der får hjælp fra sikkerhedsfirmaet CSIS Security Group og Center for Cybersikkerhed.

Udover at have låst IT-systemerne truer hackergruppen nu også med at offentliggøre tusindvis af stjålne dokumenter, hvis ikke Vestas betaler en løsesum. Det kaldes dobbeltafpresning.

Inde på det såkaldte *dark web* tikker et ur. Det viser, hvor lang tid Vestas har til at betale løsesummen.

Uret vises på en side på dark web, hvor virksomheder bliver hængt til tørre af den cyberkriminelle gruppe LockBit. Det er her, at følsomme dokumenter bliver lækket, hvis ikke virksomhederne betaler løsesummen.

Alt bliver lækket

Sammen med cybersikkerhedsfolkene håndterer Vestas selv de data, der er blevet krypteret og dermed skal genskabes fra backups. De har fra starten besluttet sig for ikke at betale de kriminelle hackere.

Hverken driften af vindmøllerne eller den daglige produktion er påvirket.

Men hackerne gør alvor af deres trussel. De begynder at offentliggøre store mængder stjålne filer fra Vestas' systemer.

Blandt dem er finansielle dokumenter, tekniske tegninger af vindmøller samt meget personlige oplysninger på centrale medarbejdere. Herunder Henrik Andersens pas.

- Jeg sidder her som direktør i Vestas, men også som privatperson. Det er jo selvfølgelig at overskride ens personlige grænse, siger Henrik Andersen og fortsætter:

- Jeg er meget bekymret og følsom over, at nogle af vores medarbejdere ser dem selv blive taget med i sådan en konflikt her. Det berører mig, fortsætter Henrik Andersen.

Hvordan kan produktion og drift blive hacket?

Udover et IT-system har virksomheder, der betragtes som kritisk infrastruktur, også såkaldte OT-systemer (Operational Technology). OT systemer styrer de industrielle maskiner.

IT og OT-systemer bør holdes adskilt, men i dag er det blevet mere almindeligt at koble dem sammen for at fjernstyre eller automatisere processerne. Det bliver kaldt det industrielle Internet Of Things (IIoT), og det er både nemmere og billigere for firmaerne at gøre det på denne måde.

Men så snart OT-systemer er koblet sammen med IT-systemer, kan hackere også potentielt komme ind.

I en del cyberrangreb rammer hackerne dog slet ikke OT-systemet, enten fordi det ikke lykkedes, eller fordi det ikke har været planen. Nogle firmaer ender dog alligevel med at lukke dele af driften, da de ikke har viden om, hvorvidt deres OT-system er ramt eller ej.

Kilder: Center for Cybersikkerhed, Søren Maigaard, direktør hos sikkerhedscenteret EnergiCERT.

Ekspert: Vi ser hundredvis af angrebsforsøg om dagen

Vestas er langt fra den eneste virksomhed i den danske energisektor, som hackere forsøger at komme igennem til.

Hos sikkerhedscenteret EnergiCERT i Kolding holder de øje med cybertrusler, der kommer ind mod cirka 100 virksomheder i Danmark indenfor fjernvarme, el og gas.

Det kan de ved hjælp af sensorer, som de har stående ude ved virksomhederne.

- Vi ser hundredvis af forsøg på angreb om dagen. I langt de fleste tilfælde fejler angrebene, fordi selskaberne har sat de rigtige sikkerhedsværn på plads. Og det er jo positivt, siger direktør Søren Maigaard.

Men hvis der pludselig opstår en fejl i sikkerheds-softwaren, og der skal foretages en opdatering, så sidder hackerne klar til at angribe. I perioden, fra fejlen opstår, til opdateringen bliver installeret, opstår der nemlig et hul:

- De kan slå til inden for minutter. Derfor bør man som virksomhed have flere forskellige forsvarsmekanismer på plads, så der altid er noget, der kan gribe ind, siger Søren Maigaard.

Selvom energisektoren er meget sårbar overfor cyberangreb, så understreger Søren Maigaard, at der tilsvarende skal meget til, før infrastruktur kan blive lagt ned.

- Der er 400 energiselskaber i Danmark, så det er en ekstremt decentralt opbygget infrastruktur. Det betyder, at du ikke bare kan hacke et enkelt selskab og så lukke landet ned. Du skal angribe et utal af selskaber, og det er meget svært at gøre.

Det holder dog ikke de cyberkriminielle, som i mange tilfælde er fra Rusland, tilbage. Ifølge Andy Greenberg er hackerne villige til at gå langt:

- Russiske hackere - både de pengeinteresserede og de statssponsorerede - har samme motiver. De vil finde et stort mål, hvor de kan lave så meget kaos som muligt. Uanset om det er at ødelægge Mærsks systemer eller ramme Vestas og tusindvis af vindturbiner rundt om i verden, så er det et utåeligt angreb.

- Enten handler det om at få virksomheder til at betale et løsesum, eller også kan det handle om at skabe kaos, fortsætter Andy Greenberg.

Vil ske før eller siden

For topchef i Vestas, Henrik Andersen, er det vigtigt, at vi som samfund tager cybertruslen mod energisektoren alvorligt.

- Jeg tror, det er vigtigt at komme til den erkendelse, at der er en ganske stigende sandsynlighed for, at du vil blive ramt af det her på et eller andet tidspunkt, siger Henrik Andersen.

Han er sikker på, at ransomware-angrebet på Vestas nu har givet medarbejderne en generel større indsigt i sikkerhed og de konsekvenser, som et enkelt forkert klik kan få:

- Vi har næsten 7000 medarbejdere i Danmark. Jeg er ikke et sekund i tvivl om, at samtlige medarbejdere nu har en noget andet forståelse for cybersikkerhed, end vi havde for blot tre måneder siden, siger Henrik Andersen.

Selvom angrebet i kroner og ører ikke har kostet Vestas tilnærmelsesvis så meget som angrebene på Mærsk, ISS og Demant, er det ikke en situation, han på nogen måde ønsker, at andre virksomheder kommer til at stå i.

- Det får du mig aldrig til at sige. Jeg kunne aldrig ønske det. Hverken at få det gentaget eller at andre får erfaringen. Når jeg kigger tilbage på det, så er det en lærerig erfaring. Men det er nok en af de dyrere købte erfaringer.