Titel	Sikkerheden starter hos medarbejderne

Brødtekst

Et verdensomspændende hackerangreb har også påvirket hverdagen i Vestforbrænding. IT har siden lørdag arbejdet intenst på at beskytte vores IT-systemer mod angreb. Det har betydet, at adgangen til nogle systemer har været midlertidig lukket ned.

Lørdag den 13. maj begyndte medierne at rapportere om et nyt hackerangreb, hvor data hos en lang række organisationer og privatpersoner blev taget som "gidsel", og der blev krævet løsesum for at frigive data igen. Angrebet er gennemført på verdensplan og har ramt store virksomheder og organisationer i mange lande.

Kunne lægge Vestforbrænding ned
Hos Vestforbrænding satte hackerangrebet også gang i en akut indsats for at sikre vores data. Siden lørdag har kollegerne i It arbejdet næsten uafbrudt – både lørdag og søndag blev hele natten også taget i brug.

- Den nye ransomware – som den type hackerangreb hedder – er farligere end dem, vi tidligere har set, fordi den ikke bare inficerer den enkelte pc, men kan sprede sig via netværket. Det betyder, at en enkelt inficeret pc i princippet kunne lægge hele Vestforbrænding ned – inklusive vores energiproduktion, siger IT-supporter Jesper Ellitsgaard.

Derfor blev der ikke taget nogen chancer. Sikring mod angreb var højeste prioritet, og det har betydet, at der har været lukket ned for adgangen til en lang række systemer i forskellige tidsrum.

- Vi sikrer os så godt vi overhovedet kan, og har iværksat en række tekniske tiltag for at minimere risikoen for, at der sker noget, selv hvis en medarbejder ved en fejl får åbnet en mail med en virus, siger systemadministrator Henrik Cortz.

It får hjælp fra en IT-sikkerhedsvirksomhed CSIS, der samarbejder med Cyber Crime Center hos Rigspolitiet.

Brugerne er den største sårbarhed
Hackerangrebet udnytter en sårbarhed i Microsofts produkter på både servere og pc'er. Det gælder også de pc'er, tablets osv., som man har derhjemme. Derfor er det også vigtigt at opdatere til nyeste version derhjemme.

For at få adgang til en pc sender hackerne typisk en mail ud med en vedhæftet fil eller et link, som brugeren opfordres til at klikke på eller downloade.

- Der bliver sendt ca. 200.000 nye virus ud hver dag, og hackerne bliver desværre dygtige og dygtigere til at lave overbevisende mails. Vi har fx lige set en mail, som angiveligt kom fra E-boks med Vestforbrændings CVR-nummer, korrekt sprogbrug og overbevisende lay-out, advarer Jesper.

Derfor er det vigtigt at alle medarbejdere er agtpågivende, selvom Vestforbrændings IT-afdeling er i højeste beredskab og har opdateret sikkerheden.

- Hvis vi tilfældigvis er de første, der bliver ramt af en ny virus, så kan vores sikkerhedssystemer ikke altid fange dem. Derfor er det ekstremt vigtigt, at alle medarbejdere er opmærksomme på ikke at åbne filer, som de ikke ved, hvad er. Man skal selvfølgelig ikke være IT-ekspert, men det er vigtigt at være kritisk og spørge os, hvis man er det mindste i tvivl, siger Henrik.

Afværget alle angreb
Indtil videre har IT heldigvis med succes afværget alle angreb. Men arbejdet med at sikre Vestforbrændings data fortsætter.

- Vi er 90% færdige med at sikre systemerne og har prioriteret det vigtigste – som har betydning for forsyning og forretningen – først, siger Jesper.

- De vitale systemer er nu oppe at køre, men vi kan ikke love, at der ikke kan komme systemafbrydelser uden varsel i kortere eller længere tid, så længe vi arbejder på at beskytte Vestforbrændings it-systemer. Det håber vi på, at der er forståelse for i organisationen, siger Henrik.

Billede: IT har sikret, at der er rigelige forsyninger af cola og flødeboller, så der er noget at stå imod med i de sene arbejdstimer, som arbejdet med at sikre Vestforbrænding mod det aktuelle hackerangreb har krævet. På billedet er det it-supporter Jesper Ellitsgaard (t.v) og systemadministrator Henrik Cortz .

Foto: Agnes Kreinøe

Udløber	01-01-2100
Afsender	Økonomi & IT
Skrevet	18-05-2017

Oprettet kl. 18-05-2017 09:29 af Agnes Jantzen Kreinøe (AJK)
Sidst ændret kl. 18-05-2017 09:39 af Morten Svarre (MOS)

Luk