Pengeafpresning via indbakken

by Mette Nielsen - torsdag, maj 01, 2014

http://perspektiv.tdc.dk/pengeafpresning-via-indbakken/

Pengeafpresning via indbakken

Betal eller vi låser virksomhedens pc'er. Sådan kan ultimatummet lyde, hvis virksomhedens systemer er blevet inficerede med ondsindet kode, og bagmændene udsætter virksomheden for afpresning.

Det kan lyde som ren fantasi fra en fjern, digital gangsterverden. Men selv helt almindelige danske virksomheder, der bevæger sig på dydens smalle sti, risikerer at blive udsat for fænomenet.
”Vi ser meget ubehagelige eksempler, hvor virksomheder ud af det blå oplever konkrete trusler om [illegible] et håndgribeligt eksempel, der stammer fra en virksomhed, som via email blev truet med DDoS-angreb.

Se eksempel på email-afpresning med trusler om DDoS-angreb

Virksomheden blev truet med DDoS-angreb og krav om at betale 10.000 dollars inden en bestemt dato [illegible] tilfælde, at et DDoS-angreb ville oversvømme og lamme virksomhedens servere. [illegible] 3000 dollars, for at

Læs også: Hvad har Zoologisk Have med DDoS at gøre?

Ransomware

Et eksempel på en anden form for afpresning har været fremme i offentligheden: Cyberkriminelle tog kontrol med computerne på en lokal politistation i den amerikanske delstat Massachusetts ved at kryptere politiets filer ved hjælp af ransomware-programmet Cryptolocker. Sagen resulterede i, at politiet valgte at betale for at få adgang til følsomme data på computerne.
Få andet meget ubehageligt eksempel er en pc-bruger, der pludselig fik et pop-up-vindue med et budskab [illegible] fundet børneporno på pc'en, og at man skulle betale et beløb for at undgå problemer.

Vigtig tendens

Udover den praktiske katastrofe man havner i ved at blive angrebet, risikerer man, at det skader virksomhedens omdømme. [illegible] hvor udbredt problemet er. Men i TDC's sikkerhedsafdeling kender man adskillige konkrete eksempler.

Den statslige varslingsinstans, DK-CERT, peger derudover på, at afpresning hører til blandt vigtige tendenser, it- og sikkerhedsansvarlige bør være opmærksomme på.

Læs DK-CERT's kommentarer om sikkerhedsudfordringer i 2014 (Computerworld).

Læs også: Om nogle år har vi ikke egne servere stående

Anbefalingen

Et vigtigt spørgsmål er; hvad skal man som virksomhed gøre, hvis man oplever at blive afpresset? Lars Højbergs anbefaling er, at man aldrig skal betale samt at man melder sagen til politiet.

"For at etablere et værn mod DDoS-angreb, er det en god idé at søge hjælp hos sin internetudbyder. Hos TDC har vi en løsning, der kører centralt i vores netværk og gør det muligt at fjerne den ondsindede trafik og kun lade den legitime passere igennem til virksomhedens servere. På den måde sikrer vi, at virksomhedens netværk og servere ikke bliver oversvømmet," forklarer Lars Højberg.

Bliver man derimod afpresset ved hjælp af ransomware-programmet Cryptolocker, ser det mere sort ud. "Jeg vil aldrig opfordre til, at man betaler kriminelle bagmænd. I det konkrete tilfælde med Cryptolocker kan man være nødt til at geninstallere sin maskine og benytte sig af den backup, man forhåbentlig har sikret sig."

Afpresning i den digitale verden foregår på flere måder – enten ved at angrebene gennemføres, eller med trusler om det:

- DDoS-angreb:
  Virksomheden trues via email med DDoS-angreb, der vil lamme virksomhedens hjemmeside og evt. andre systemer.
- Cryptolocker:
  Virksomhedens computere krypteres af denne eller andre slags ransomware, så man ikke kan få adgang til sine egne systemer eller data.
- Pop up-vindue:
  Brugere får inficeret deres pc'er og bliver mødt med pop up-vinduer, der kommer med beskyldninger og trusler.
- Uopfordret support:
  Medarbejdere ringes op af en påstået Microsoft-tekniker, som skal løse et teknisk problem, hvorefter vedkommende lokker medarbejderen til at klikke på et link, der installerer virus. Herefter afpresses virksomheden til at betale for et antivirusprogram, som reelt er ren fup.

Link: Så meget koster cyber-kriminalitet os hvert eneste år