Spørgsmål & Svar - Hackerangreb

Som de fleste ved, blev vi for nyligt ramt af et hackerangreb i LIFA A/S. I samme øjeblik hackerangrebet blev konstateret, blev nogle af Nordens førende IT-specialister indenfor dette område – Truesec – tilknyttet, og siden da har de stået for hele det efterfølgende forløb.

Nedenfor har vi oplistet de oftest stillede spørgsmål, som vi er stødt på undervejs samt givet svarerne hertil.

Spørgsmål:	Svar:
Hvordan opdagede I, at I var blevet hacket?	Søndag d. 27. februar var der nogle medarbejdere, der prøvede at arbejde, men de kunne ikke komme på vores drev. Derfor kontaktede de vores IT-afdeling, og gjorde opmærksom på dette. Vores IT-afdeling undersøgte straks, hvad årsagen var, og i den forbindelse kunne de konstatere, at noget var galt, og at det lignede et hackerangreb. De foretog derfor en kontrolleret nedlukning, og kontaktede vores forsikringsselskab samt meldte det til politiet. Vores forsikringsselskab reagerede med det samme ved at sende de eksterne sikkerheds- og gendannelsesspecialister, Truesec ud til os. De har stået for processen med at få os op at køre igen lige siden.
Ved I med sikkerhed hvem der angreb jer?	Det var den russiske hackergruppe Conti, der stod bag angrebet. Den måde hackerne ønsker at kommunikere, er via Contis egne platforme, så derfor er vi sikre på, at det er dem. Den måde de arbejder, og de programmer og scripts de bruger, passer også overens med, hvad Conti har gjort i andre bekræftede angreb.
Ved I hvorfor de angreb netop LIFA?	Nej, vi har ingen dialog haft med hackerne, så vi ved ikke, hvorfor de angreb netop LIFA. Angrebet på LIFA ligner dog en typisk ransomware-operation, og vi kan indtil videre ikke se tegn på forsøg på at tilgå systemer med vigtig information. Vi kan heller ikke se, at de har søgt efter informationer af denne art. Vores eksterne sikkerhedseksperter fra Truesec arbejder til daglig med netop denne type angreb, og har alene sidste år rykket ud til mere end 170 cyberangreb i Skandinavien heraf mange ransomware-angreb. De ser ingen indikationer på, at dette angreb skulle være andet end et "normalt" ransomware-angreb, og Truesec ser ingen direkte relationen til konflikten i Ukraine.
Har hackerne opkrævet løsesum?	Da der er tale om et ransomware-angreb, har de givet instruktioner på, hvordan en dialog skal indledes. Men da vi som nævnt ikke har haft – eller ønsker at have – dialog med dem, har vi ikke fulgt op på dette, og kender derfor heller ikke beløbets størrelse.
Ved I hvordan de er kommet ind?	Vi arbejder pt efter formodningen om, at angriberne er kommet ind via en sårbarhed i et eksternt system, som en sårbarhedsscanning foretaget af en ekstern leverandør desværre har overset.

Ved I hvilke data, der er blevet kompromitteret?	Det er uklart hvilke data, om nogen overhovedet, der er blevet tilgået direkte af angriberne.
Ved I om nogle data er blevet lækket?	Pt. er der ikke konstateret læk af nogle data, og vi følger dette nøje. I den kommende periode vil vi dog tilkøbe en ekstern service, som overvåger om nogle af vores data lækkes. Dermed bliver vi i stand til at reagere øjeblikkeligt, såfremt vi får kendskab til, at vores data er lækket.
Er der nogen risiko ved at bruge jeres IT-løsninger eller udveksle data med jer fremadrettet?	Nej. Alle vores IT-løsninger samt data er blevet gendannet og efterfølgende gennemgået af eksterne sikkerhedseksperter således, at vi er sikre på, at ingen af vores IT-løsninger eller data forsat er inficeret.
Kan I garantere, at I ikke bliver hacket igen?	Det kan man desværre aldrig garantere. For selvom vi har arbejdet meget seriøst med IT-sikkerhed i LIFA igennem længere tid, så lykkedes det alligevel hackerne at komme uden om vores foranstaltninger. Vi kan dog garantere, at det vil være endnu sværere at hacke LIFA fremadrettet, for vi kommer naturligvis til at bruge angrebet til noget konstruktivt internt. Vi kommer nemlig til at tage ved lære af dette angreb, og se hvordan vi kan styrke vores IT-sikkerhed yderligere.
Er I oppe og køre igen?	Størstedelen af vores forretning er oppe og køre igen, og de IT-løsninger der forsat ikke er i drift, forventer vi er oppe og køre i løbet af uge 10 (med enkelte undtagelser). Det kan dog ikke undgås, at der fremadrettet vil opstå situationer, hvor vi støder på problemer med manglende data etc., som er blevet slettet ifm. angrebet. Når disse situationer opstår, håber vi på vores kunders forståelse og hjælpsomhed, men det er vi dog fortrøstningsfulde omkring, for den opbakning vi indtil videre har oplevet fra kunder, samarbejdspartnere etc. har været enorm! Hele vejen rundt har der været fuld forståelse for den situation, vi desværre er havnet i, for alle kan se, at vi blot er et uskyldigt offer, som er blevet ramt af noget, der kunne ramme – og løbende rammer – mange danske virksomheder uanset branche og størrelse.

Hvis der er nogle, der har yderligere spørgsmål til noget forretningsmæssigt i LIFA ift. angrebet, så er I velkomne til at kontakte adm. direktør i LIFA, Thomas Boding, på tbo@lifa.dk

Hvis der derimod er yderligere spørgsmål af sikkerhedsteknisk karakter, så er i meget velkomne til at kontakte Truesec, Morten von Seelen, som kender detaljerne i efterforskningen.