Virus på PC'en

En dag-til-dag egenopplevelse

Å få datamaskinen infisert eller få alle filer på datamaskinen slettet, er ikke et spørsmål om «hvis»;men NÅR.

Før jul var det en mengde personer og firmaer hvor nettopp dette skjedde: Det kom en epost fra Posten som sa: Vi har forsøkt å levere en pakke til deg, men kunne ikke levere. Følg linken for å spore pakken». For mange av oss er det ikke noen bombe at Posten ikke kan levere. Dessuten venter de fleste av oss en pakke før jul, og med Posten kan vi forvente at vi må følgfe ekstra opp.

I tillegg var undertegnede stresset; vi ventet på pakke, og midt i hastverket trykket vi oss videre for å få vite hvor pakken var…

Og under over alle undere; vi gikk altså rett i fellen, og oppdaget det ikke før alle filene på tilkoplede maskiner på kontoret, var uleselige.

Hva gjør man når katastrofen inntrer, og realiteten er at man hverken har trent på situasjonen eller har 100% kontroll på sikkerhetsrutiner?

Da mørket senket seg, bokstavelig talt, ble jeg helt svett: Dersom jeg hadde mistet alt, var det bare å legge ned firmaet. Jeg ringte min tidligere systemerer/ dataansvarlig, etter ca 1 time. Han ble selvfølgelig forskrekket, men holdt hodet kaldt og sa:

"Skru av og trekk ut nettkabel fra alle maskiner på kontoret, bortsett fra PC'en som var hovedmaskinen: Den var grundig infisert så der var ikke mye å gjøre. Gjennom telefonkontakt startet vi arbeidet for å se omfanget av skaden: Vi fant at at 80% av filene var sikkerhetskopiert til Dropbox, men 20% manglet totalt.

Jeg kontaktet Dropbox, beskrev situasjonen og kunne vente svar i løpet av 4-5 dager.

På min maskin lå det igjen en beskjed fra kaprerne: Betal løsepenger, ellers vil du aldri se filene dine igjen. Og hvis du forsøker å tukle med antihacking, vil filene ikke kunne bli hentet tilbake.

Det ble forsøkt «alt»; lastet opp programmer, ned og opp og app; alle metoder ble tatt i bruk. Fikk bekreftet at dette var et smart virus, ikke mulig for noen å låse opp. Jeg var i seng langt på natt

Dag 2: Vi fikk selvfølgelig ikke gjort annet enn operasjon «redde data»: Våre programmerere hadde kontakt med Kaspersky, et ledende antivirus programhus. Men der var vi ikke kunder, og alt var vanskelig…

I mellomtiden hadde jeg funnet ut at de fleste viktige filer for produksjon av Focus, var borte. Og de fleste private bilder, minner, you name it, som lå på harddiskene, var kryptert: Et voldsomt arbeid bare for å få Focus på beina.

Gjennom kontakter fikk vi laget en kort liste over institusjoner i Norge som kunne hjelpe. For vi var vel ikke de eneste som hadde gått på smellen?

Vi ringte Datatilsynet: Men de var ikke en slik instans, må vite.

Vi ringte til NORSIS. DE var landets «Men in Black» - men svarte ikke på telefon. Så vi sendte en epost.

Dag 3: Jeg begynte å bli hysterisk. Ringte tilbake til NORSIS: Jeg fikk kontakt, og etter å ha bli satt over noen ganger, fikk jeg en hyggelig person som forklarte at de ikke kunne hjelpe med dette viruset. (Det virket som om han ikke riktig hadde peil heller). «Good luck og klar deg sjæl». Men han fikk sagt at betale løsepenger, det måtte jeg ikke gjøre, for det er å oppmuntre til at kriminell handling lønner seg.

Kvelden kom; og natten. Da fant jeg at det var verd å prøve å betale kidnapperne av filene mine, som forlangte bitcoins til en ca verdi NOK kr 5000. Så jeg startet en møysommelig prosess med å få kontakt med kidnapperne via en hemmelig site som jeg måtte laste ned en spesiell webleser. Men jeg fikk kontakt og fikk instruksjoner: Rene detektivfilmen dette her.

Dag 4: Startet morgenen med å finne bitcoinselgere, og det ble en spesiell øvelse med en forholdsvis ærlig nordmann som solgte bitcoinsene til markedsverdi lik ca NOK 6.500; men det fikk gå. Men hjelpsom var selgeren overfor en komplett uvitende meg.

fortsetter....

Prosessen ble satt i gang, og etter noen timer mottok jeg «antidot» for viruset. Imens hadde to egne programmerere arbeidet for å finne botemiddel, men uten resultat: Det var jo en risk for at dersom vi tuklet for mye på egenhånd, så ville filene mine bli avlivet.

Fortsetter neste side

Jeg startet på ettermiddagen, og det ble en møysommelig jobb. Glemte jeg å fortelle at jeg har ca 1,4 millioner filer samlet opp etter 1980? Og starten var mistrøstig: Jeg kjørte anti-filene noen ganger, uten å se resultat. Men så oppdaget jeg at jeg måtte ta én og én hovedmappe av gangen (men av og til også undermappene separat). Utpå natten så jeg lyset: Flere og flere filer dekryptert; de kom frem en etter en….

Dag 5: Motet kom tilbake; jeg brukte hele dagen på å organisere, kopiere til backup, til sikre steder, til minnepinner og hva det nå enn var. Og filene kom sakte men sikkert tilbake til meg.

Resultat: I hvertfall 80% av de 20% jeg ikke hadde backup på, og som var viktige, ble reddet, og til dags dato har jeg kanskje savnet en eller tre filer.

Hva lærte jeg ?

Når ulykken først er ute, er du alene:

Jeg synes det er på sin plass å ta et oppgjør med NORSIS som via sine nettsider forteller om alt de gjør og hvor viktige de er, hvor tilstede de skal være for å redde norske bedrifter og arbeidsplasser. I en dypt fortvilet situasjon for meg og firmaet, ble jeg glatt avvist og overlatt til meg selv. Detaljer ligger på Tannhjulet.no, bare søk «NORSIS»

Det jeg ikke var alene om, var å gå på limpinnen. Jeg har hørt at Legeforeningens interne datasystem var nede i 2 dager, og jeg hørte i ettertid fra to forretingsforbindelser som begge fikk alle filene kryptert. Den ene reddet alle, og den andre de fleste. Jeg tror mange betaler hvis de er paniske nok og de tror det nytter, men felles er at vi sjelden får høre om det.

Det jo litt flaut….

Jeg slapp altså med skrekken, og betalte NOK 6500 for en kraftig og viktig voksenopplæring.

Hva må jeg formidle videre?

I utgangspunktet var sikkerhetsplanene på plass; Jeg skulle «bare» vente til jul med å komplettere sikkerhetssystemene. Men det tok altså ikke hackerne hensyn til, og jeg gikk på flausen med «posten» som beskrevet innledningsvis.

Om du bruker en datamaskinen ganske mye og har mange filer; dokumenter og bilder på et datamedium, så må du vurdere hva mine råd er. Jeg har ingen provisjoner for noe, men jeg velger å være spesifikk slik at du bare kan løpe og kjøpe de nødvendige ting.

Det er ikke er snakk om hvis, men når, at noen lykkes med å hacke datamaskinen din.

Bruk derfor ikke mange ressurser på å lagre filer på forskjellige steder: minnepinner, CD, DvD, hardisker eller på å ta manuelle backupper….. Du oppdager fort at hvis du bare har mange nok filer forskjellige steder, så finner ingen igjen det man gjerne ville finne..

Du gjør så her:

1. Kjøp et abonnement på www.dropbox.com – 1 TB lagringsplass inkludert versjonshistorikk og backup. Dropbox synkroniserer alle filene mellom sitt datalagringsmedium og en eller flere datamaskiner du bruker. Pris pr nå er kr. ….. årlig
2. Last alle filene dine opp til Dropbox
3. Sørg for at en av datamaskinene dine har en harddisk som rommer ALLE filene dine. Det letter en senere backup.
4. Kjøp og installér Kaspersky virusprogram. Det kan lønne seg å kjøpe fra et amerikansk nettsted.

Bonus: Voksenopplæring

- Dropbox har en vidunderlig synkroniseringsfunksjon som gjør at du får tak i alle dine filer over alt.
- Kaspersky anti-virus gir deg muligheten til å sikre betalinger, dine passord og dine ID-opplysninger
- Google's "GoogleDocs" berøres ikke.

Hvem: Legeforeningen, leverandør av maskiner

Google docs var ikke berørt

KURS senere? Ønsker: NORSIS Hadde tydeligvis «samarbeidende parter» som skulle profilere seg…deres reklameres det med, En typisk norsk statsdrevet institusjon, Gjemmekontor og flotte flosker som politikere eller bevilgende myndigheter skal tro på.