SJU TIPS FOR Å FOREBYGGE RANSOMWARE

Skadelig programvare som krypterer dataene dine og ber om løsepenger for å dekryptere dem, har blitt svært populære de siste årene. Formålet med denne programvaren er å presse ofrene for penger mot å gjenopprette de krypterte dataene.

Som andre datavirus kan ransomware trenge seg inn på en enhet ved å benytte seg av sikkerhetshull i sårbar programvare eller ved å lure noen til å installere programmet. Ransomware angriper viktige instanser som sykehus, offentlige skoler og politiavdelinger.

Nå har de også funnet veien til hjemmedatamaskiner.
Når det gjelder ransomware er det flere ting du bør og ikke bør gjøre.

Ransomware har vist seg å være en lukrativ industri for kriminelle. Gjennom årene har dens dårlige omdømme ført til at politimyndighetene nå samarbeider med internasjonale myndigheter for å identifisere og rettsforfølge svindlere.

Mesteparten av ransomware-angrepene som har funnet sted tidligere, har vært knyttet til ansattes dårlige beskyttelsesvaner.

1. ***IKKE BETAL LØSEPENGENE.*** Det vil bare oppmuntre og finansierer de aktuelle angriperne. Selv om du betaler løsepengene, er det ingen garanti for at du får tilgang til filene dine igjen.
2. ***GJENOPPRETT EVENTUELLE BERØRTE FILER FRA EN KJENT GOD SIKKERHETSKOPI.*** Den raskeste metoden for å få tilgang til filene dine igjen er ved å gjenopprette dem fra en sikkerhetskopi.
3. ***IKKE OPPGI PERSONOPPLYSNINGER*** når du svarer på e-postmeldinger, uønskede telefonanrop, tekstmeldinger eller direktemeldinger. Nettfiskere vil prøve å lure ansatte til å installere skadeprogrammer eller starte angrep ved å hevde at de er fra IT-avdelingen. Ta alltid kontakt med IT-avdelingen dersom du eller dine kollegaer mottar mistenkelige anrop.
4. ***BRUK ANERKJENTE ANTIVIRUSPROGRAMMER OG EN BRANNMUR.*** Det er svært viktig at du har en sterk brannmur og holder sikkerhets-programmene oppdatert. Det er viktig å bruke antivirus-programvare fra et anerkjent selskap på grunn av alle de falske programmene som finnes.
5. ***BRUK INNHOLDSSØK OG FILTRERING PÅ POSTSERVERNE DINE.*** Innkommende e-postmeldinger bør gjennomsøkes for å se etter kjente trusler, og eventuelle vedleggstyper som kan utgjøre en trussel, bør blokkeres.
6. ***KONTROLLER AT ALLE SYSTEMER OG PROGRAMMER ER OPPDATERT MED RELEVANTE OPPDATERINGER.*** Utnyttingsverktøy som finnes på kompromitterte nettsteder, brukes ofte til å spre skadeprogrammer. Regelmessig oppdatering av sårbar programvare er nødvendig for å forhindre infeksjon.
7. ***HVIS DU ER UTE OG REISER, BØR DU VARSLE IT-AVDELINGEN PÅ FORHÅND,*** spesielt hvis du skal bruke offentlig WiFi. Pass på at du benytter et pålitelig VPN (Virtual Private Network) når du bruker offentlig WiFi, for eksempel Norton WiFi Privacy.

Ransomware-kriminelle angriper ofte små og mellomstore bedrifter. Ransomware er en kriminell aktivitet som enkelt kan unngås ved å bruke de ovennevnte løsningene. Norton Security Premium, kombinert med opplæring i disse truslene, er en utmerket beskyttelsesplan for dagens nettmiljøer.