OUCH! | August 2014

Det Månedlige Nyhetsbrevet om Sikkerhetsbevissthet for Databrukere

OUCH!

I DENNE UTGAVEN...

- Hva er kryptering?
- Kryptering av stillestående informasjon
- Kryptering av informasjon i transitt

Kryptering

Hva er kryptering?

Du har kanskje hørt folk bruke ordet "kryptering" og hvordan du burde bruke det for å beskytte deg selv og din informasjon. Problemet er at konseptet kryptering kan være forvirrende. Kryptering kan heller ikke beskytte deg mot alle trusler, det har sine begrensninger. I dette nyhetsbrevet vil vi med enkle ord forklare hva kryptering er, hvorfor du bør bruke det og hvordan du implementerer det riktig.

Gjesteredaktør

Christopher Crowley (**@CCrowMontance**; **+ChrisCrowley**) er en konsulent som holder til i Washington, DC. Han er hovedinstruktør for SANS-kurset Mobile Device Security and Ethical Hacking (SEC575) og forfatter av Incident Response Team Management (MGT535).

Du har ufattelig mye sensitiv informasjon på dine enheter, for eksempel finansielle dokumenter, bilder, e-post og medisinske journaler. Hvis en av dine enheter skulle bli mistet eller stjålet, så kan all denne sensitive informasjonen bli aksessert av hvem enn det er som har fysisk tilgang til enheten. I tillegg utfører du kanskje sensitive transaksjoner på enheten, som nettbank eller netthandel. Hvis en angriper kan monitorere dine aktiviteter på nett, så kan de stjele informasjonen din og få tilgang til finansielle kontoer eller kredittkortnummer. Kryptering beskytter deg i disse tilfellene ved å sørge for at uautoriserte personer ikke kan aksessere eller modifisere informasjonen.

Når informasjon ikke er kryptert er det kalt klartekst. Det betyr at hvem som helst kan enkelt lese eller aksessere informasjonen. Kryptering konverterer denne informasjonen til et ikke-lesbart format. Kryptering fungerer ved å bruke komplekse matematiske operasjoner og en unik nøkkel for å konvertere informasjonen til kryptert tekst. Nøkkelen er det som låser eller låser opp informasjonen, på samme måte som en nøkkel kan låse eller låse opp en dør. Et vanlig eksempel på en nøkkel er et passord, bare de som vet passordet kan dekryptere og aksessere informasjonen. For å beskytte informasjonen må du beskytte nøkkelen. Kryptering består av to hovedkategorier, kryptering av stillestående data (som data lagret på PC-en) og data i bevegelse (som når du sender data til en nettside).

Kryptering av stillestående informasjon

Hovedmålet med å kryptere statisk informasjon er å beskytte informasjonen selv om mobilen eller datamaskinen blir mistet eller stjålet. Femten år siden var ikke dette noe problem, de fleste datamaskiner var store klunkete stasjonære

Kryptering

enheter som det var vanskelig å flytte på. Dagens bærbare PC-er veier bare et par kilo, mens mobiltelefoner ligger nærmere 100 gram. Disse enhetene er kraftige og inneholder store mengder med informasjon, men de er også lette å miste. I tillegg, har man andre mobile medier som kan holde sensitiv informasjon, som USB-minnepinne og CD ROM. En vanlig metode for kryptering av informasjon på disse mediene er full-disk kryptering. Det betyr at all informasjon på enheten er kryptert, du trenger ikke å bestemme hvilken informasjon som burde krypteres. De fleste moderne operativsystemer kommer innebygd med støtte for full-disk kryptering, men du må skru det på. Mac OS X for eksempel har FileVault, noen versjoner av Windows har Bitlocker. Hvis din datamaskin støtter full-disk kryptering vil vi anbefale å skru det på. De fleste mobiltelefoner støtter også full-disk kryptering. iOS, operativsystemet brukt i iPhone og iPad, tar i bruk full-disk kryptering når du har satt en passkode. For å finne ut om din PC eller mobiltelefon støtter full-disk kryptering, spør brukerstøtte eller overordnete. Hvis det er din personlige PC, kontakt produsenten eller sjekk dokumentasjonen.

Kryptering er en kraftig måte å sikre informasjon på, men den er ikke sterkere enn nøkkelen.

Kryptering av informasjon i transitt

Informasjon er også sårbar når den sendes over til noen andre. Hvis dataen ikke er kryptert, kan den bli fanget opp av andre. Dette er grunnen til at du bør sørge for at sensitiv kommunikasjon, som nettbank, e-post og kanskje til og med bruk av sosiale medier er kryptert. Den mest brukte formen kryptering er HTTPS. Dette betyr at all trafikk mellom din nettleser og nettjeneste er kryptert. Se etter https:// i adressefeltet, det merkes ofte på andre måter også, som ved bruk av grønn farge eller hengelås. Dette er tegn på at kommunikasjonen er kryptert, noen nettlesere viser alle tre. Hvis du bruker et offentlig trådløst nettverk, sørg for at du alltid bruker kryptering når det er mulig. Sørg også for at e-postklienten er satt opp til å bruke en kryptert tilkobling. De fleste e-postklienter støtter kryptering, internettleverandør kan kanskje også hjelpe deg med å skru på kryptering på e-postklienten.

Implementere kryptering korrekt

Uansett hvilken type kryptering du bruker eller hvordan du bruker det, nesten alle krypteringsmetoder deler noen felles steg man må ta for å bruke det sikkert.

Kryptering

- Krypteringen er ikke sterkere enn nøkkelen. Hvis noen greier å gjette eller kompromittere nøkkelen, så vil de ha tilgang til dataene dine. Du må beskytte nøkkelen.
- Hvis du bruker en passkode eller et passord som nøkkel, sørg for at det er et langt, sikkert passord og ikke glem det. Hvis du glemmer passordet, så vil du miste dataene.
- Du må også beskytte datamaskinen, hvis angripere kan ta kontroll over datamaskinen, kan de også omgå krypteringen. Sørg derfor for at mobiltelefonen og PC-en er sikker.
- Hvis du har flere valg for kryptering, velg den sterkeste metoden.

Les Mer

Abonner på månedlig OUCH! nyhetsbrev om sikkerhetsbevissthet, se gjennom OUCH! arkivene og lær mer om SANS sine programmer for sikkerhetsbevissthet hos http://www.securingthehuman.org.

Norsk Versjon

NorSIS er en del av regjeringens helhetlig satsing på informasjonssikkerhet i Norge. NorSIS jobber for at informasjonssikkerhet skal bli en naturlig del av hverdagen. Les mer på www.norsis.no.

Ressurser

Mac OS X FileVault: http://support.apple.com/kb/HT4790?viewlocale=no_NO

iOS kryptering: http://support.apple.com/kb/HT4175?viewlocale=no_NO&locale=en_US

Android kryptering: http://www.androidauthority.com/how-to-encrypt-android-device-326700/

Windows kryptering: http://windows.microsoft.com/en-us/windows/protect-files-bitlocker-drive-encryption#1TC=windows-7

Sikre datamaskinen: http://www.securingthehuman.org/ouch/2012#december2012

Passordhåndterere: http://www.securingthehuman.org/ouch/2013#october2013

Redaksjon: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis