Thomas Malmberg
är en informationssäkerhetskonsult
som driver företagen Mint Security
och Hackrfi.

Allas ansvar att personlig information skyddas

Datasäkerhet, informationssäkerhet, cybersäkerhet ... ett tråkigt barn har många namn. Tråkigt därför att vi oftast hamnar i kontexten kring informationssäkerhet då det gäller någonting negativt. Allt från skådespelerskan Kaley Cuocos läckta nakenbilder till dataintrånget på terapiklinik-en Vastaamo till spionaget på Utrikesministeriet. Om vi någon gång hittar en positiv kontext kring informationssäkerhet – då blir det riktigt urtråkigt.

Då vi nu nästan med vetenskaplig noggrannhet fastställt att informationssäkerhet ligger på en skala från tråkigt till riktigt urtråkigt ska vi försöka gräva oss ut ur träsket. För oss som jobbar inom området är det helt klart intressant – en passion. För en utomstående kan det dagliga arbetet beskrivas som en blandning av byråkrati och arkeologi. Saker ska utföras och bokföras till punkt och pricka. Utförs det inte till punkt och pricka, leder det till att saker ska undersökas. Undersökningen ska ske med arkeologisk pietet. Men på samma sätt som vi – icke-arkeologer – litar på att arkeologen putsar sina artefakter med en tandborste ska ni – icke informationssekretörer – kunna lita på att specialisterna inom området sköter saker noggrannt och med pietet.

Då du betalar på internet ska inte ditt kreditkortsnummer stjälas, läggas på en lista av verifierade nordiska kreditkort för att sedan återförsäljas i paket av 10 000 på en underjordisk marknadsplats i dark net. Kreditkortsnummer säljs i ”bulk” och den som säljer dessa får betalt oberoende av om numren fungerar eller icke. Ifall man kan garantera att en stor procent av korten fungerar, blir priset högre. Kan man köpa in och ”bundla” personinformation med korten, höjs enhetspriset markant.

Låter detta som en komplicerad businessmodell med många olika slags nivåer av specialister där

”Då du betalar på internet ska inte ditt kreditkortsnummer stjälas, läggas på en lista av verifierade nordiska kreditkort för att sedan återförsäljas i paket av 10 000 på en underjordisk marknadsplats i dark net.”

envar lägger till sitt mervärde – och tar ett arvode? Visst. Dagens moderna cyberkriminalitet följer på många nivåer samma businessmodeller som vanlig legitim affär och handel.

Vad händer med din information?

Låter det redan lite intressant? Bra. Då ska vi tala om ansvar. I dagens samhälle är det som vi vet viktigt att vi har en massa rättigheter. Rätt att göra det ena och rätt att göra det andra. Och alla andra har plikter. Plikter att se till att saker fungerar så att vi kan utöva våra rättigheter. Inom informationssäkerhet finns det lagar, paragrafer, direktiv och förordningar (sådär till att börja med) för hur saker ska skötas. Vi behöver inte veta så mycket om detaljerna däri. I många fall har vi nog helt rätt och slätt rätt att anta att saker fungerar på ett sätt som gagnar oss.

Men hur långt sträcker sig detta? Finska statliga och kommunala tjänster – den offentliga sektorn? Den privata lokala sektorn – med vilken man har gjort något slags kontrakt (tänk exempelvis banker, biljettaffärer, resebyråer, spelsajter…) – där ska gälla liknande spelregler.

Men hur fungerar detta med motsvarande parter utanför våra gränser? Vad händer med din personliga information då du ansöker om visum till ett land långt borta? Eller köper biljetter till en konsert i landet långt borta? Det kan vara helt olika spelregler. Helt olika ansvar. Ansvaret ligger nödvändigtvis inte på huruvida din information skyddas, utan kring huruvida din information görs tillgänglig för ”tredje parter”.

Jag måste också tala om sociala medier. Inga sociala medier eller liknande tjänster är gratis. Alla kostar din information. Personlig information och en uppdaterad profil är valutan. Kommer du ihåg hur ett enstaka kreditkortsnummer inte var värt så mycket, men kopplat med personlig information ändras värdekedjan? Ingen bryr sig väl om att jag har en katt eller tar en selfie med mitt favoritklädmärke varje dag? Förutom att det kanske betyder att mitt kreditkort i kredikortbolagens automatiska ”fraudscoring-system” med större sannolikhet fungerar bra i affärer där man säljer dessa kläder – eller kattmat.

Givetvis är modellen en hel del förenklad – men ni förstår säkert poängen och modellen av hur jag tänker. Eftersom man gratis givit bort en full profil av sig själv – en profil som i dagens ”big data”-värld är betydligt mer komplex än en skjorta och en katt – vet de sociala medierna ibland mera om dig själv än du själv vet.

Informationen kan säljas till alla som betalar

I framtiden kanske du kan fråga din Högtalare där hemma (som du givetvis på förhand givit lov att lyssna på allt du säger) – ”Hej Högtalaren, är min fru gravid?”. Då din Högtalare innehåller fulla profiler av flere miljarder individer och deras beteendemönster inom livets alla områden, kan Högtalaren med mycket stor sannolikhet berätta svaret åt dig. Och svaret är garanterat rätt. Om man nu vill hitta något positivt kring detta, så är det väl bäst att lägga in ett ”Hej Högtalaren, beställ hem blommor och choklad sedan då min fru är gravid” på förhand. För säkerhets skull liksom.

Men jag har ju ett bra lösenord. Min mormors namn och födelsedatum – och hon är så gammal att INGEN kan komma ihåg det. Vi ska tala om lösenord, men först måste det klargöras att det inte är bara dessa omtalade informationsläckor från sociala medier som utgör något slags hot (ifall man upplever det att ens personliga liv och profil är offentliga som ett hot – alla gör ju inte det). Användarvillkoren ger en möjlighet för Högtalaren och dess gelikar att helt enkelt använda sig av den information du lägger in i den på just ett sådant sätt som gagnar dem – som att till exempel sälja informationen vidare till alla som betalar för den. Många köper och betalar. Och hur informationen sedan används, det har vi över huvud taget ingen kontroll över.

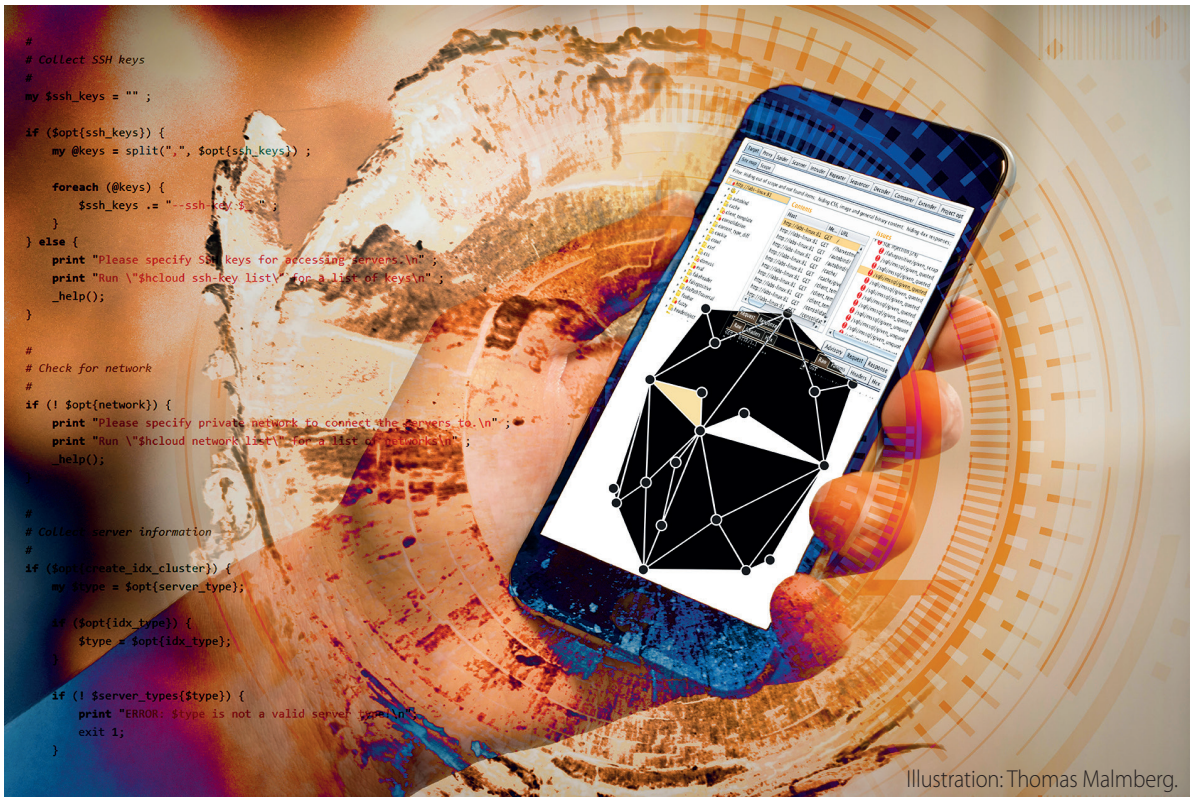

Illustration: Thomas Malmberg.

Återanvänd aldrig lösenord

Lösenordet då. Lösenordet räddar oss inte. Ett bra lösenord tar oss en liten bit framåt. Bra och unika lösenord tar oss en rejäl bit framåt. Flere faktorer – en dialog i telefonen du måste klicka dig vidare från för att få tillgång – där ligger dagens sanning. Med betoning på ordet dagens – detta är inte nödvändigtvis morgondagens sanning.

I Finland är vi lyckligt skattade då vi använt flerfaktor-autenticering längre än någon annan. Ni kommer ihåg de där papperslapparna man skulla gömma i bordslådan och gräva fram en gång per månad då telefonföreningens räkning skulle betalas. Vi är vana vid att använda ett sådant system.

Dagens system är givetvis en applikation i mobilen, inga papperslappar. Men principen är densamma. Ifall du råkar tappa bort ditt lösenord så att någon annan får reda på det är det oanvändbart utan denna andra ”faktor”. Och detta fungerar. Så vi repeterar lite om lösenord.

1) Återanvänd ALDRIG lösenord. Då ett lösenord komprometteras (du eller någon annan slarvar bort det) är alla tjänster du använt samma lösenord på i riskzonen. Det är ett stort arbete att gå igenom alla tjänster och byta lösenord – och kanske omöjligt att ens komma ihåg alla tjänster.

2) Använd lösenord som är lätta att komma ihåg, men (matematiskt) svåra att cracka (crackning är en metod att maskinellt bryta ner ditt lösenord). Matematiskt-algoritmiskt sett är *”kla)(88_”* ett sämre lösenord än *”Min-Häst-Har-En-4-Meter-Lång-Svans-Som-Heter-Brunte”*. Du kan själva avgöra vilket som är lättare att komma ihåg.

3) Använd flerfaktor-autenticering. De flesta relevanta tjänster ger dig möjlighet att koppla på något slags flerfaktor-autenticering. Alla ”flere faktorer” är inte lika bra, men faktum är att de alla är bättre än att bara använda användarnamn och lösenord.

4) Använd ett program för att hantera dina lösenord. Ett skilt program som specialiserar sig på att spara lösenord på ett säkert sätt och dessutom hjälper dig att generera lösenord, har en backup på dina lösenord – och möjliggör att du har dina lösenord med dig i alla dina olika mobileneheter. Mycket bra. Använd några timmar

"Använd ett program för att hantera dina lösenord. Ett skilt program som specialiserar sig på att spara lösenord på ett säkert sätt och dessutom hjälper dig att generera lösenord."

nästa veckoslut för att installera och lära dig använda detta – och lär familjen på samma gång. Betala också några euro för kalaset.

Nummer 4 kan med fördel också användas till annat än lösenord. Ni kommer ihåg hur vi sparade vår pinkod till kreditkortet i vår Nokia 3330. Smart – år 2000. År 2021? Vad händer med din pinkod då du äntligen får en inbjudan till diskussionsappen Clubhouse – den inbjudan du väntat på tålmodigt i åtminstone flere minuter redan? Priset för att få använda Clubhouse är att du laddar upp din adressbok till tjänsten. Den där addressboken där Pelle Svanslös telefonnummer är 2276. Inte så svårt att gissa att ett fyrsiffrigt telefonnummer är en pinkod.

Så nu har någon läckt ut ditt kreditkortsnummer, du har skänkt bort din profil via Högtalaren och till slut donerat din pinkod. Jag började med att tala om ansvar – på vems ansvar var detta?

Ansvar för alla som kommunicerar

Så kom ihåg, sköt om dina lösenord. Dina lösenord är en nyckel till din dagbok och låset på din toalett. Lösenorden skyddar inte bara dig utan också dina närmaste. Du har kanske inget att dölja, men du har ett ansvar för alla andra som kommunicerar med dig. Då jag stänger min dörr, min dator, min telefon vill jag kunna anta att jag får vara för mig själv. Utan att någon tittar eller lyssnar. Likaväl ska detta gälla för dig. För oss alla.

Thomas Malmberg var presentatör på Ekonomiska samfundets och Fintech Finlands diskussionsmöte på distans om datasäkerhet och dess ekonomiska effekter 2.2 2021. Länken till mötet finns på Ekonomiska samfundets hemsida, www.ekonomiskasamfundet.fi.