Dags för cybersäkerhetsekonomi

ULRIK FRANKE

nr 2 2022 årgång 50

Digitaliseringen öppnar nya möjligheter för hela samhället. Både privat och offentlig sektor har under de senaste decennierna utvecklat nya digitala arbetssätt. Det är en utveckling som dels ger möjlighet att göra *samma saker* snabbare och effektivare, dels möjlighet att göra *helt nya saker* som tidigare var omöjliga. Potentialen är alltså mycket stor, även om det inte alltid är självklart vare sig hur vi bäst ska kunna dra full nytta av den (se exempelvis Breman och Felländer 2014 samt Ekman 2019) eller hur produktivitetsförbättringar till följd av digitalisering och automatisering rätteligen bör mätas (Maican och Orth 2018). Klart är emellertid att digitaliseringen är här för att stanna. Vi arbetar, studerar och umgås på nya sätt i dag jämfört med för ett par decennier sedan och covid 19-pandemin har ytterligare påskyndat den utvecklingen.

Detta medför emellertid inte bara nya möjligheter, utan även nya svårigheter. Ständigt kommer nyheter om cyberincidenter, såväl oavsiktliga misstag och olyckor som avsiktliga angrepp. Ett axplock från de senaste åren inkluderar osäker lagring av körkortsuppgifter och patientjournaler, avbrott i tjänster som Bank-ID, Swish och kortbetalningar och uppmärksammade fall av utpressningsvirus. Det sistnämnda fenomenet fick kanske sitt genombrott i det allmänna medvetandet under 2021; först med angreppet på Colonial Pipeline i maj som allvarligt påverkade drivmedelsförsörjningen på hela den amerikanska östkusten och sedan med REvil-angreppet i juli som i Sverige stängde ner hundratals Coop-butiker. Dessvärre är detta sakernas tillstånd regel snarare än undantag: Det finns inget som tyder på att incidenterna kommer att avta i framtiden. Det är allvarligt, eftersom säkra och pålitliga tjänster är en förutsättning för att uppnå digitaliseringens fördelar. Vare sig autonoma industrirobotar, självkörande bilar eller innovativa *fintech*-tjänster kan leva upp till sin potential om de ständigt drabbas av avbrott eller om angripare lätt kan manipulera dem.

Cybersäkerhet betraktas ofta som ett rent tekniskt problem. Attacksimuleringar, AI-baserad spaning efter misstänkt aktivitet och bättre kryptografi är exempel på tekniska lösningar som får stor uppmärksamhet. Otvivelaktigt är sådan teknikutveckling viktig och har potential att ge oss säkrare system. Men cybersäkerhet är inte *enbart* ett tekniskt problem. Säkerheten, eller bristen därpå, uppstår när en mänsklig användare nyttjar tekniken i ett organisatoriskt och ekonomiskt sammanhang. Det betyder att bättre cybersäkerhet också kan uppnås på andra sätt än genom tekniska åtgärder.

2006 introducerade Anderson och Moore ämnet informationssäkerhetsekonomi (*economics of information security*) i en inflytelserik artikel i *Science*. De argumenterar övertygande för att grundorsakerna till många informations- och cybersäkerhetsproblem går att förstå utifrån nationalekonomi. Varför investerar företag inte tillräckligt i säkerhet? Därför att den som sprider skadlig kod eller orsakar driftavbrott för andra inte bär hela kostnaden. Molntjänster och integrationslösningar kopplar samman moderna IT-miljöer så att fakturor, ordrar, saldon, mätvärden etc ständigt flödar mellan olika aktörer. Detta ökar produktiviteten, men möjliggör samtidigt att såväl avbrott som skadlig kod kan spridas på samma sätt. Bristande säkerhet hos någon utsätter alla för risk (se exempelvis Dieye 2020 för en empirisk studie av spridningseffekter av cyber-

Ulrik Franke, tekn dr, är senior forskare vid RISE Research Institutes of Sweden och affilierad fakultet vid KTH. Hans forskning handlar bl a om cyberförsäkringar och kostnader för cyberincidenter. ulrik.franke@ri.se

angrepp). Under sådana omständigheter är det naturligtvis fortfarande värt att investera en del i säkerhet, men knappast att bekosta stora säkerhetsinvesteringar hos alla andra som man är hopkopplad med, med risken att någon av dessa ändå klantar till det. Den här sortens resonemang är ett starkt argument för att det troligen investeras för lite i cybersäkerhet (se exempelvis Gordon m fl 2014 men notera att Acemoglu m fl 2016 nyanserar bilden). Cybersäkerhetsbrister är kort sagt *negativa externaliteter*, precis som utsläpp av föroreningar.

Varför konkurreras inte sårbar eller opålitlig programvara ut av bättre alternativ? Anderson och Moore svarar att det beror på att det är nästan omöjligt för köparna att skilja säker och osäker programvara åt. Då varken kan eller vill de betala extra för säkerhet. Marknaderna för nästan alla digitala tjänster lider alltså av *asymmetrisk information* på samma sätt som Akerlofs (1970) berömda begagnade bilar. Därmed blir betalningsviljan för säkerhet låg och incitamentet för säljaren att utveckla säkra produkter mindre. Liksom med de begagnade bilarna finns det förvisso mekanismer som kan mildra effekterna av informationsasymmetrin, exempelvis garantier (Woods och Simpson 2018) eller varumärken: Stora mjukvaruföretag med starka varumärken har ganska mycket att förlora på att sälja osäkra produkter eftersom de vill sälja till köpstarka kunder över lång tid. Men för små och nystartade mjukvarutillverkare kan det tvärtom vara tillväxtstrategiskt rationellt att skjuta säkerheten på framtiden: Först skapa en produkt och få kunder, sedan (om det bär sig) försöka göra den säkrare.

Det är den här sortens belysande resonemang som får Anderson och Moore att dra slutsatsen att dålig säkerhet minst lika ofta uppstår på grund av dåliga incitament som på grund av dålig design. Om de har rätt i det så betyder det i sin tur att lika mycket kraft och forskningsmöda borde läggas på att studera och åtgärda dåliga incitament som på att studera och åtgärda dålig teknisk design. Sådan forskning är inte bara akademiskt intressant utan också praktiskt användbar: Moore (2010) argumenterar för att ganska små interventioner som justerar incitament och korrigerar uppenbara marknadsmisslyckanden kan få stor positiv effekt på cybersäkerheten i ett land. Det kan i så fall vara avsevärt billigare än stora teknikprojekt för att uppnå motsvarande säkerhetsökning.

Tyvärr har de cybersäkerhetsekonomiska frågeställningarna ännu inte väckt så mycket uppmärksamhet bland svenska forskare (några undantag finns; se Hermelin m fl 2014 och Franke 2020). Kanske beror det på att området ligger mitt emellan olika akademiska discipliner och kräver teknikintresserade ekonomer eller ekonomiintresserade teknikvetare (som undertecknad) – kanske helst bådadera – för att bli givande. Hursomhelst finns det all anledning för fler nationalekonomer att intressera sig för cybersäkerhet. Några exempel på spännande forskningsfrågor, helt utan anspråk på att vara uttömmande, är följande:

Vad kostar egentligen cyberincidenter? Det är inte svårt att hitta braskande rapporter om höga incidentkostnader, men det finns påtagliga metodproblem (se Florêncio och Herley 2013) och Anderson m fl 2013) och många av dem som gör undersökningar av incidentkostnader har sina egna agendor (Moore 2010). Inte ens lagstadgad obligatorisk incidentrapportering i enlighet med EU:s NIS-direktiv tycks ge kostnadsdata av särskilt god kvalitet (Franke m fl 2021).

När borde cyberincidenter offentliggöras? Utifrån resonemanget om asymmetrisk information ovan kan det vara rimligt att ställa krav på att incidenter offentliggörs, så att marknaden får mer

information om vilka produkter som är säkra respektive osäkra. Bilden kompliceras dock av att offentliggörande av incidenter inte bara ger mer information till köpare och säljare, utan också till illasinnade angripare. Huruvida angripare eller försvarare gynnas mest är en öppen fråga (Anderson 2007) och varje sorts offentliggörande måste därför noga utvärderas på sina egna meriter.

Hur hänger cybersäkerhet ihop med konkurrens och marknadskoncentration? Geer m fl (2020) illustrerar pedagogiskt problemet: Å ena sidan finns det goda skäl att tro på *skalfördelar* inom cybersäkerhet: Ett litet företag som knappt ens har en IT-ansvarig på heltid har uppenbarligen inte råd att hålla sig med en cybersäkerhetsexpert. Å andra sidan finns det också anledning att tro på *skalnackdelar* inom cybersäkerhet. För det första är stora bolag ofta mer attraktiva måltavlor för riktade angrepp, eftersom det finns mer att stjäla där. För det andra är system med många användare ofta stora, komplicerade och ständigt under vidareutveckling. Därmed blir de svåra att överblicka och hålla säkra. Själva komplexiteten blir en säkerhetsrisk – en tydlig skalnackdel. Vilken tendens som väger över i vilka sammanhang är en spännande empirisk fråga.

Vilken roll kan och bör försäkringsbranschen spela i cybersäkerhetssammanhang? Säkerhetsexperten Bruce Schneier menade entusiastiskt redan för tjugo år sedan att ”i framtiden kommer försäkringsbranschen att styra datorsäkerhetsbranschen” (Schneier 2001, s 114). Det som talar för den tesen är att försäkringsbolag är experter på riskhantering, att de kan göra stora risker hanterbara genom att sprida dem på många aktörer och att de kan använda premiesättningen för att skapa incitament för kunderna att bli mer säkra. Men medan vi har tillförlitlig och mer eller mindre heltäckande statistik över trafikolyckor, bränder och översvämningar har vi ingen motsvarande bra statistik över cyberincidenter. Det betyder att cyberförsäkringspremierna kan vara för höga eller för låga – ingen vet säkert (se exempelvis OECD 2020 och Franke 2017 för ett svenskt perspektiv). Warren Buffett dömde 2018 ut branschen med omdömet att ingen riktigt vet vad de ger sig in på när de ställer ut cyberförsäkringar.

Hur ska vi leta efter sårbarheter effektivt? Allt fler mjukvaruutvecklande företag belönar dem som rapporterar sårbarheter i deras produkter (*bug bounty*) och minskar därmed frestelsen att i stället utnyttja dem för egen vinning (Magazinius m fl 2019). Men att utforma sårbarhetsbelöningsprogram är inte helt lätt, bl a eftersom olika program konkurrerar med varandra om sårbarhetsjägarnas uppmärksamhet (Maillart m fl 2017).

Dessa – och andra – cybersäkerhetsekonomiska frågeställningar har den gemensamma nämnaren att de både är akademiskt intressanta och praktiskt relevanta. Nationalekonomer har mycket att bidra med för att göra dagens och morgondagens digitaliserade samhälle säkrare. Det är dags för cybersäkerhetsekonomi!

REFERENSER

Acemoglu, D, A Malekian och A Ozdaglar (2016), ”Network Security and Contagion”, *Journal of Economic Theory*, vol 166, s 536–585.

Akerlof, G A (1970), ”The Market for ’Lemons’: Quality Uncertainty and the Market Mechanism”, *Quarterly Journal of Economics*, vol 84, s 488–500.

Anderson, R och T Moore (2006), ”The Economics of Information Security”, *Science*, vol 314, s 610–613.

Anderson, R (2007), ”Open and Closed Systems Are Equivalent (That Is, in an Ideal World)”, i Feller, J, B Fitzgerald, S A Hissam och K R Huff (red), *Perspectives on Free and Open Source Software*, MIT Press, Cambridge MA.

Anderson, R m fl (2013), ”Measuring the Cost of Cybercrime”, i Böhme, R (red), *The Economics of Information Security and Privacy*, Springer, Berlin och Heidelberg.

Breman, A och A Felländer (2014), ”Diginomics – nya ekonomiska drivkrafter”, *Ekonomisk Debatt*, årg 42, nr 6, s 28–38.

Dieye, R, A Bounfour, A Ozaygen och N Kammoun (2020), ”Estimates of the Macroeconomic Costs of Cyber- attacks”, *Risk Management and Insurance Review*, vol 23, s 183–208.

Ekman, B (2019), ”Är Sverige på väg att missa e-hälsotåget?”, *Ekonomisk Debatt*, årg 47, nr 7, s 62–66.

Florêncio, D och C Herley (2013), ”Sex, Lies and Cyber-Crime Surveys”, i Schneier, B (red), *Economics of Information Security and Privacy III*, Springer New York, New York NY.

Franke, U (2017), ”The Cyber Insurance Market in Sweden”, *Computers & Security*, vol 68, s 130–144.

Franke, U (2020), ”Cybersäkerhet för en uppkopplad ekonomi”, Entreprenörskapsforum, Stockholm.

Franke, U, J Turell och I Johansson (2021), ”The Cost of Incidents in Essential Services – Data from Swedish NIS Reporting”, i Percia David, D, A Mermoud och T Maillart (red), *Critical Information Infrastructures Security. CRITIS 2021*, Springer, LNCS 13139, Springer, Cham.

Geer, D, E Jardine och E Leverett (2020), ”On Market Concentration and Cybersecurity Risk”, *Journal of Cyber Policy*, vol 5, s 9–29.

Gordon, L A, M P Loeb, W Lucyshyn och L Zhou (2014), ”Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model”, *Journal of Information Security*, vol 6, artikel 52952.

Hermelin, J, H Karlzén och P Nilsson (2014), ”Informationssäkerhet och ekonomi”, Tekn rapport FOI-R--3927—SE, FOI Totalförsvarets forskningsinstitut, Stockholm, https://www.foi.se/rapportsammanfattning?reportNo=FOI-R--3927--SE.

Magazinius, A, N Mellegård och L Olsson (2019), ”What We Know about Bug Bounty Programs – An Exploratory Systematic Mapping Study”, i Groß, T och T Tryfonas (red), *International Workshop on Socio-Technical Aspects in Security and Trust*, LNCS 11739, Springer, Cham, https://doi.org/10.1007/978-3-030-55958-8_5.

Maican, F och M Orth (2018), ”Digitalisering, strukturomvandling och produktivitet i tjänsteföretag”, *Ekonomisk Debatt*, årg 46, nr 1, s 47–58.

Maillart, T, M Zhao, J Grossklags och J Chuang (2017), ”Given enough Eyeballs, all Bugs Are Shallow? Revisiting Eric Raymond with Bug Bounty Programs”, *Journal of Cybersecurity*, vol 3, s 81–90.

Moore, T (2010), ”The Economics of Cybersecurity: Principles and Policy Options”, *International Journal of Critical Infrastructure Protection*, vol 3, s 103–117.

OECD (2020), ”Enhancing the Availability of Data for Cyber Insurance Underwriting: The Role of Public Policy and Regulation”, https://www.oecd.org/finance/insurance/Enhancing-the-Availability-of-Data-for-Cyber-Insurance-Underwriting.pdf.

Schneier, B (2001), ”Insurance and the Computer Industry”, *Communications of the ACM*, vol 44, s 114–115.

Woods, D W och A C Simpson (2018), ”Cyber-warranties as a Quality Signal for Information Security Products”, i Bushnell L, R Poovendran och T Başar (red), *Decision and Game Theory for Security. GameSec*, LNCS 11199, Springer, Cham.