KRIMI KIBERNETIK, SFIDË PËR SHOQËRINË E SOTME

revista monitor numer: 0277 faqe nr: 24
Autor: Igli Tashi

Krimi kibernetik është një fenomen që prek një sërë kompetencash, si ato në fushën e informatikës, kriminologjisë, ekonomisë, drejtësisë

Përdorimi i teknologjive të reja të informacionit1 dhe veçanërisht i Internetit ka marrë një rëndësi të veçantë në jetën e përditshme. Ky fenomen prek jo vetëm aktivitetet e një organizmi qoftë ai shtetëror apo privat, i implikuar në sferën e biznesit apo të një aktiviteti jo fitimprurës, por mund të prekë dhe njeriun e thjeshtë në aktivitetin e tij të përditshëm, në sferën e tij private apo profesionale. Si çdo teknologji e re e vënë në dispozicion të një numri të madh përdoruesish, Interneti paraqet jo vetëm të mira dhe përfitime, por në të njëjtën kohë dhe një sërë problemesh. Duke qenë një teknologji "e liberalizuar" prej disa kohësh, siç përdoret në zhargon, nuk ia vlen të zgjatemi në diskutimin e përfitimeve që sjell përdorimi i kësaj teknologjie. Anën e përfitimeve mund ta përmbledhim për momentin në një frazë të vetme: komunikim (në kuptimin e gjerë të fjalës) i shpejtë, i pakushtueshëm dhe tërësisht i pavarur nga nocioni i distancës.
Në këtë artikull do të përqendrohemi kryesisht në shmangien që i bëhet qëllimit primar të përdorimit të kësaj teknologjie (komunikimit). Keqpërdorimi i saj nga elementë kriminalë njihet me emrin krim kibernetik (cybercrime). Në praktikën e përditshme konstatohen dy lloj sjelljesh përballë fenomenit të krimit kibernetik. Në njërën anë, kemi përdoruesin e përditshëm, i cili udhëhiqet shumë shpesh nga ideja që "e keqja shkon gjithmonë tek të tjerët". Në anën tjetër, kemi specialistët e fushës që udhëhiqen diametralisht nga e kundërta, domethënë që "të tërë jemi të barabartë, të paktën në terma matematike, ndaj probabilitetit të të qenit objekt i një sulmi kriminal". Ndryshe nga përdoruesi i zakonshëm, specialisti i kushton kohë analizës së fenomenit për të kuptuar funksionimin e tij. Duhet theksuar fakti që në asnjë moment dhe në asnjë rrethanë nuk duhet të biem pre e idesë që një ditë këtë probabilitet mund ta bëjmë zero. Ky pohim merr një rëndësi të madhe kur ka të bëjë për më shumë me teknologjitë e reja dhe me sigurinë informatike. Nga natyra, teknologjitë e reja janë në evolucion të vazhdueshëm dhe për rrjedhojë dhe rreziqet e lidhura me këtë teknologji evoluojnë në të njëjtën mënyrë. Scott Peck, një psikiatër i njohur amerikan dhe autor i suksesshëm librash shkruan: "E vetmja mënyrë për të pasur siguri në jetë është të njohësh pasigurinë".

Jo thjesht krim informatik
Pra, ç'është krimi kibernetik, nga vjen, çfarë e ndihmon të jetë kaq i përhapur, si mundemi ta parandalojmë dhe a jemi të përgatitur përballë këtij fenomeni? Këto janë disa pyetje që specialistët, qofshin këta informaticienë, specialistë të sistemeve të informacionit, kriminologë, juristë, ekonomistë etj., mundohen t'i trajtojnë në aktivitetin e tyre të përditshëm. Në fakt, krimi kibernetik duhet distancuar pak nga një nocion i përgjithshëm i asaj që quhet krimi informatik. Ky i fundit lidhet me një aktivitet kriminal që ka si objekt apo si mënyrë të kryerjes së krimit, kompjuterin. Krimi kibernetik, pra, është në këtë prizëm një nënkategori e krimit informatik dhe ka të bëjë me veprimtarinë kriminale të zhvilluar në rrjet (network). Interneti është një nga rrjetet më globalë dhe më të përdorur sot. Pas këtij saktësimi mundemi të evidentojmë që qenia në rrjet na ekspozon ndaj rrezikut të një sulmi të mundshëm. Do të ishte joprofesionale këshilla e një shkëputjeje nga rrjeti, sepse në strukturën

ekonomike të sotshme gjithnjë e më shumë globale, shkëputja do të shndërronte organizmin në një njësi jokonkurrente.
Një aspekt tjetër që duhet trajtuar për të kuptuar fenomenin e krimit kibernetik, është dhe teknologjia e përdorur. Një përdoruesi të zakonshëm kompjuteri apo Interneti, që nga momenti që çdo gjë funksionon normalisht për të, nuk i intereson më se çfarë veprimesh, përllogaritjesh apo protokollesh kryen kompjuteri për të arritur në këtë rezultat. Nga ana tjetër, prodhuesit e programeve, pajisjeve, ISP2 etj., nuk është se kanë një vullnet spontan të informojnë përdoruesin mbi mënyrën e funksionimit dhe për të qenë të arsyeshëm kjo gjë do të ishte irrealiste. Pra si përfundim, teknologjia mbetet pak a shumë jotransparente për përdoruesin.
Përsa i përket Internetit, disa faktorë të tjera bëjnë që kjo teknologji të jetë e cënueshme dhe për rrjedhojë një terren shumë fertil për zhvillimin e krimit.
Nga një këndvështrim teknologjik mund të përmendim faktin që Interneti është një teknologji publike dhe e hapur për të tërë. Historikisht, rrjeti komunikues u zhvillua si një mjet i fushës ushtarake për t'u përdorur më pas nga universitarët për të lehtësuar komunikimin ndërmjet tyre. Ky vizion mbi përdorimin bëri që në fillesat e saj, teknologjia e Internetit të mos përfshinte aspektin e sigurisë përderisa komunikimi (si në rastin ushtarak, ashtu dhe në atë universitar) bëhej ndërmjet njerëzve që njiheshin dhe që kishin besim te njëri-tjetri. Teknologjia e Internetit është një teknologji "best effort". Kjo do të thotë që në konceptimin e saj "bëmë atë çka mundëm" për të arritur në rezultatin e dëshiruar, pa imagjinuar se çfarë devijimi mund t'i bëhej përdorimit të tij.
Nga një këndvështrim i rrjetit dhe i sistemit, në rastin e Internetit kemi të bëjmë me një liri të madhe përsa i përket konfigurimit, mënyrës së trajtimit segmentar të sigurisë dhe ç'është më e rëndësishme në rastin tonë, mungesës totale të kontrollit. Jo më kot Interneti identifikohet si "rrjeti i rrjeteve" dhe shpesh struktura e tij krahasohet me rrjetën e merimangës.
Nga një këndvështrim legal, Interneti është i konceptuar dhe funksionon në një mënyrë të tillë, që për të nocioni i kufijve nuk ekziston. Në fushën juridike një krim në radhë të parë sanksionohet nga një ligj. Ky ligj i përket një shteti të caktuar dhe zbatohet nga një gjykatë kompetente e një shteti të caktuar. Nocioni i shtetit është i lidhur ngushtë me nocionin e territorit, pra me kufijtë shtetërorë. Kjo ndikon shumë në fazën e përndjekjes së krimit. Imagjinoni një pirat informatik që kryen aktin e tij kriminal nga Kina le të themi, duke sulmuar një bankë në Zvicër dhe duke derdhur shumën e vjedhur elektronikisht në Itali. Cili institucion gjyqësor dhe cili ligj është kompetent në këtë rast? Kina, vendi nga i cili autori kreu krimin; Zvicra, vendi ku ndodhet viktima; apo Italia, vendi ku u realizua rezultati? Tre vende kaq të ndryshme përsa i përket vendndodhjes, kulturës juridike dhe perceptimit të nocionit të krimit a do të munden të bien dakord për përndjekjen dhe gjykimin e këtij akti? Përgjigjja nuk është shumë e evidente.
Së fundmi, në qoftë se konsiderojmë problemin nga një këndvështrim i përdoruesit, atëherë kemi prekur thembrën e Akilit. A është përdoruesi i ndërgjegjshëm për pasojat që mund t'i sjellë përdorimi i Internetit? Përgjigjja është negative në më të shumtën e rasteve.

Edhe bankat të prekura
Në një emision të transmetuar së fundmi në një nga televizionet shqiptare, një drejtues banke solli si argument faktin që programet bankare janë aq të sofistikuara sa është shumë e vështirë të "thyhen", gjë që paraqet një pjesë të së vërtetës. Në momentin që operacionet bankare kryhen në rrjet, siç është dhe rasti i 'e-banking', i cili po fillon të praktikohet dhe në Shqipëri, përdoruesi është i cënueshëm pavarësisht nga forca dhe algoritmet e përdorura në programet e bankës. Ka dhe një fakt tepër të rëndësishëm që duhet theksuar: krimi do të kërkojë të godasë viktimën më të dobët, më të papërgatitur, pra shënjestrën më tërheqëse për të. Eksperienca na tregon që mbi 50% e sulmeve kanë si objekt personin. Por edhe nëse marrim në konsideratë organizmin e bankës më vete dhe faktin

e programeve të sofistikuar, eksperienca në fushën e krimit kibernetik ka treguar se mbi 70% e sulmeve kanë zanafillë të brendshme. Kjo mund të vijë nga një vartës i pakënaqur, një vartës i prirur thjesht nga përfitimi etj. Lista e motivimeve është e gjatë. Në këtë aspekt kompleksiteti teknologjik nuk ndihmon shumë dhe është struktura administruese e institucionit dhe gjithë aspektet përbërëse të saj që marrin një rëndësi të veçantë. Në emisionin në fjalë u soll si shembull me të drejtë niveli i kontrollit shumë rigoroz mbi personelin që njihet si "administrimi nëpërmjet frikës" (fear management). Por në të njëjtën kohë rezultatet e kësaj strategjie janë shumë të diskutueshme në rrethet e profesionistëve të burimeve njerëzore. Për mendimin tonë, duke konsideruar shkallën e lartë të rëndësisë së sistemeve të informacionit në mbarëvajtjen dhe mbijetesën e organizmit, do kishim anuar më shumë në një stil administrimi të përqendruar mbi komunikimin, edukimin dhe sensibilizimin e vartësve mbi pasojat si në nivel personal, ashtu dhe atë profesional. Kjo, duke shpjeguar se teknologjia nuk mundet të zgjidhë e vetme problemet që lidhen me sigurinë informatike dhe me krimin informatik dhe që faktori njerëzor ka një rëndësi të rangut të parë.

Teoria e trekëndëshit

Për t'iu rikthyer nocionit të krimit kibernetik dhe për të kuptuar atë që quhet modus operandi të kryerjes së krimit duhet t'i referohemi teorisë së trekëndëshit që citohet shpesh në literaturën e kriminologjisë. Kjo teori na tregon se për të kryer një krim duhet që në të njëjtën kohë të kemi një bashkërendim të tre faktorëve: të një krimineli të motivuar, të një objekti vulnerabël, të cilët ndodhen në të njëjtin vend, në të njëjtën kohë. Duke u nisur nga kjo teori dhe duke konsideruar elementët që cituam më sipër:

n njohjen e kufizuar të Internetit nga ana e përdoruesit;

n motivimin, mundësinë dhe lehtësimet që kanë kriminelët për të kryer aktin kriminal nëpërmjet Internetit;

n vendin e takimit ideal dhe konstant siç është rrjeti;

mund të nxjerrim përfundimin, që krimi kibernetik është dhe do të bëhet gjithnjë e më shumë një terren shumë tërheqës për kriminalitetin. Praktika tregon që krimi i organizuar ka kuptuar tashmë rëndësinë dhe përfitimin nga fenomeni i krimit kibernetik. Anonimiteti që ofron Interneti, bën që krimi i organizuar po fillon dalëngadalë të interesohet dhe të marrë në dorë frenat e këtij fenomeni. Si shembull, mund të marrim rastin e Bankës së Siçilisë në vitin 2000, ku një grup prej 20 personash, natyrisht me njohuri specifike në fushën e informatikës dhe të lidhur me disa familje mafioze, arritën të krijonin një klon të servisit 'e-banking' të bankës. Kështu, arritën në këtë mënyrë të përvetësonin shumën prej 400 milion $ të vëna në dispozicion nga Komuniteti Europian për zhvillimin rajonal. Pasi përvetësuan shumën në fjalë, ata përdorën servise të tjera bankare 'on-line' për t'i pastruar këto para dhe për të humbur gjurmët duke implikuar banka të njohura si Bankën e Vatikanit, disa banka në Zvicër dhe në Portugali3. Në këtë fazë duhet theksuar dhe fakti që për të mos rënë në sy, shumat e përvetësuara nga krimi kibernetik, janë në më të shumtën e rasteve, shuma të vogla parash. Sipas raportit IC3 2004 Internet Fraud – Crime Report4, 43% e shumave të përvetësuara nuk janë më shumë se 100 $ për akt dhe 25.6% nuk e kalojnë 1000$. Pra, është shumë e vështirë për të tërhequr vëmendjen e specialistëve apo për të justifikuar një procedurë gjyqësore.

Është e kuptueshme që një artikull nuk mund të trajtojë në detaj gjithë përbërësit e fenomenit të krimit kibernetik. Mesazhi, i cili deshëm të përcillnim, është që krimi kibernetik është një fenomen që prek një sërë kompetencash, si ato në fushën e informatikës, kriminologjisë, ekonomisë, drejtësisë etj. Krimi kibernetik është pra, një fenomen kompleks dhe e vetmja mënyrë për t'i bërë ballë do të ishte një mënyrë globale e trajtimit të problemit. Për këtë duhet një bashkëpunim i gjithë ekspertëve të fushave të sipërpërmendura për të shmangur zgjidhjet segmentare. Për këtë është e rëndësishme të konceptojmë një arkitekturë globale të sigurisë së informacionit që të marrë në konsideratë brenda saj dimensionin teknik dhe operacional, dimensionin juridik dhe rregullator, dimensionin organizativ dhe ekonomik, duke mos harruar dimensionin

njerëzor.