ISSN 2181-3187

AXBOROT XAVFSIZLIGIGA TAHDIDLARNI BAHOLASH VA PROGNOZLASH AMALIYOTI

Anvarova Muqaddas Xomidjon qizi
O‘zbekiston jurnalistika va ommaviy kommunikatsiyalar universiteti
Xalqaro jurnalistika yo'nalishi 3- kurs talabasi

Annotatsiya: Axborot xavfsizligiga tahdidlarni bashorat qilish tashkilotlar tobora murakkab va doimiy kibertahdidlarga duch kelayotgan bugungi raqamli landshaftda muhim vazifa hisoblanadi. Ushbu dissertatsiya axborot xavfsizligiga tahdidlarni prognoz qilishning metodologiyalari, muammolari va real misollarini o'rganib, potentsial xavflarni yumshatishda proaktiv choralar muhimligini ta'kidlaydi.

Kalit so’zlar: Axborot xavfsizligi, proaktiv choralar, prognoz, tahdid.

Axborot xavfsizligiga tahdidlarni baholash va prognozlash bugungi raqamli landshaftda muhim amaliyot bo'lib, tashkilotlar sirli ma'lumotlarni buzishi, operatsiyalarni buzishi mumkin bo'lgan tobora murakkablashgan kibertahdidlarga duch kelmoqda. Axborot xavfsizligiga tahdidlarni baholash zaifliklarni aniqlash, xavflarni baholash va kamaytirish strategiyalariga ustuvorlik berish uchun mo'ljallangan turli metodologiya va tizimlarni o'z ichiga oladi. Keng qo'llaniladigan tizimlardan biri Milliy Standartlar va Texnologiyalar Instituti (NIST) tomonidan ishlab chiqilgan NIST Cybersecurity Framework. Ushbu asos tashkilotlarga tahdidlarni toifalarga ajratish, joriy imkoniyatlarni baholash va xavflarni boshqarish tamoyillari asosida nazoratni amalga oshirish orqali kiberxavfsizlik holatini boshqarish va yaxshilash uchun tizimli yondashuvni taqdim etadi.

Yana bir yondashuv Threat Intelligence bo‘lib, u tashkilot tizimlari va ma’lumotlariga qaratilgan joriy va potensial tahdidlarni tushunish uchun ma’lumotlarni yig‘ish va tahlil qilishni o‘z ichiga oladi. Tahdid razvedkasi manbalariga ochiq manbali razvedka (OSINT), qorong'u veb monitoringi va kiberxavfsizlik agentliklari bilan hamkorlik kiradi. Tashkilotlar paydo bo'ladigan tahdidlarni, zaifliklarni va hujum vektorlarini ulardan foydalanishdan oldin faol ravishda aniqlash uchun tahdid razvedkasidan foydalanadilar.

Bryus Shnayerning 2000-yilda chop etilgan “Sirlar va yolg‘onlar: Tarmoqqa ulangan dunyoda raqamli xavfsizlik” nomli asosiy asari kiberxavfsizlik sohasida asosiy manba bo‘lib qolmoqda. Ushbu kitobda Shnayer axborot xavfsizligining murakkab

ISSN 2181-3187

manzarasini o'rganadi va tobora o'zaro bog'langan raqamli muhitda tahdidlarni baholash va prognoz qilish amaliyotiga e'tibor qaratadi[1].

Schneier raqamli xavfsizlik kontekstida tahdidlarni baholash konsepsiyasini shakllantirishdan boshlaydi. Uning ta'kidlashicha, tahdidlarni samarali baholash nafaqat tizimlar yoki dasturiy ta'minotdagi zaifliklarni aniqlash, balki potentsial raqiblarning motivlari, imkoniyatlari va uslublarini yaxlit tushunishni talab qiladi. Tahdid qiluvchilar moliyaviy daromad olishga intilayotgan shaxsiy xakerlardan tortib, siyosiy yoki strategik maqsadlarni ko‘zlayotgan murakkab milliy davlat aktyorlarigacha bo‘lishi mumkin[2].

Schneier tahdidlarni bir nechta alohida turlarga ajratadi, ularning har biri axborot xavfsizligi uchun o'ziga xos muammolarni keltirib chiqaradi:

1. Texnik zaifliklar: Bular tajovuzkorlar tomonidan ishlatilishi mumkin bo'lgan dasturiy ta'minot, apparat yoki tarmoq konfiguratsiyasining zaif tomonlarini o'z ichiga oladi. Hujumchilar noma'lum yoki tuzatilmagan kamchiliklarni nishonga oladigan nol kunlik ekspluatatsiyalar kabi zaifliklar proaktiv xavfsizlik choralari va tezkor javob protokollarining muhimligini ta'kidlaydi[3].

2. Inson omillari: Shnayer xavfsizlikni buzishda inson xatosi va zararli insayder tahdidlarning rolini ta'kidlaydi. Ijtimoiy muhandislik taktikasi, masalan, shaxslarni maxfiy ma'lumotlarni oshkor qilish uchun manipulyatsiya qiladigan fishing hujumlari kiberxavfsizlikdan xabardorlikni oshirish bo'yicha kuchli treninglar va siyosatlarga ehtiyoj borligini ko'rsatadi.

3. Milliy-davlat aktorlari: Davlat homiyligidagi kiberjosuslik va kiberurush muhim va rivojlanayotgan tahdidlar manzarasini ifodalaydi. Milliy davlatlar tomonidan tashkil etilgan ilg'or doimiy tahdidlar (APT) muhim infratuzilmani, davlat idoralarini yoki xususiy korxonalarni nishonga olib, milliy xavfsizlik va iqtisodiy barqarorlikka jiddiy xavf tug'dirishi mumkin.

Tahdidlarni baholashning murakkabligini tasvirlash uchun Shnayer kiberxavfsizlik landshaftini shakllantirgan real voqealarga tayanadi:

- Stuxnet (2010): Qo'shma Shtatlar va Isroil tomonidan ishlab chiqilgan deb hisoblangan murakkab kiber qurol, Stuxnet Eron yadroviy inshootlarini nishonga olgan. Ushbu hujum kiber imkoniyatlarning geosiyosiy keskinliklar bilan kesishishini

[1] Smith, B., Williams, L. Using SQL Hotspots in a Prioritization Heuristic for Detecting All Types of Web Application Vulnerabilities. In: O’Conner, L. (Ed.), Proceedings of the 2011 IEEE Fourth International Conference on Software Testing, Verification and Validation. IEEE Computer Society, March 21-25, Berlin, Germany, 2011. pp. 220–229.

[2] Ozment, A. Software Security Growth Modeling: Examining Vulnerabilities with Reliability Growth Models. In: Gollmann, D., Massacci, F., Yautsiukhin, A. (Eds.), Proceedings of the First Workshop on Quality of Protection. Vol. 23 of Advances in Information Security. Springer Boston 790 Massachusetts, September 19-22, Como, Italy, 2006. pp. 1–13

[3] Roumani, Y., Nwankpa, J. K., Roumani, Y. F. Time Series Modeling of Vulnerabilities. Computers & Security. 2015. P. 51.

ISSN 2181-3187

ta'kidladi va jismoniy infratuzilmani buzish uchun kiberoperatsiyalar potentsialini namoyish etdi.

- Equifax Data Breach (2017): Tarixdagi eng yirik ma’lumotlar buzilishidan biri bo‘lgan Equifax hodisasi kompaniya veb-ilovasidagi zaiflik tufayli millionlab shaxslarning shaxsiy shaxsiy ma’lumotlarini fosh qildi. Buzg'unchilik ma'lumotlar buzilishi natijasida tashkilotlar duch keladigan moliyaviy sohaga e'tibor qaratdi va mustahkam xavfsizlik amaliyoti va tartibga rioya qilish muhimligini ta'kidladi.

Kiberxavfsizlik texnologiyalari va metodologiyalaridagi yutuqlarga qaramay, tahdidlarni to'g'ri baholash va prognoz qilishda bir qator muammolar mavjud:

1. Tahdid landshaftining murakkabligi: Kiberxavfsizlik tahdidi landshafti dinamik va murakkab bo‘lib, tahdid subyektlari o‘zlarining taktika, texnika va tartiblarini (TTP) doimiy ravishda rivojlantirmoqda. Ushbu murakkablik yangi hujum vektorlari va zaifliklarni kutishni qiyinlashtiradi.

2. Ma’lumotlar hajmi va tezligi: AT tizimlari va tarmoqlari tomonidan yaratilgan ma’lumotlarning katta hajmi tashkilotlarni to‘sib qo‘yishi mumkin, bu esa shovqin va haqiqiy tahdidlarni farqlashni qiyinlashtiradi. Bundan tashqari, tahdidlarning tarqalish tezligi real vaqt rejimida yoki real vaqtda tahlil qilish imkoniyatlarini talab qiladi.

3. Malakatlar yetishmovchiligi: tahdidlarni samarali tahlil qilish va ularga javob berish tajribasiga ega kiberxavfsizlik bo‘yicha mutaxassislarning global tanqisligi mavjud. Bu tanqislik tashkilotlarning ichki tahdidlarni ishonchli baholash imkoniyatlarini saqlab qolish qobiliyatini cheklaydi.

4. Xavfsizlik vositalarining integratsiyasi: Ko'pgina tashkilotlar bir nechta xavfsizlik vositalari va echimlaridan foydalanadilar, ularning har biri o'ziga xos ogohlantirishlar va ma'lumotlar to'plamini yaratadi. Ushbu vositalarni birlashtirish va tahdidlar manzarasining yagona ko'rinishini ta'minlash uchun ma'lumotlarni o'zaro bog'lash muhim muammodir[4].

5. Muvofiqlik va me'yoriy talablar: sanoat qoidalari va ma'lumotlarni himoya qilish qonunlariga muvofiqligi tahdidlarni baholash amaliyotiga murakkablik kiritadi. Tashkilotlar maxfiy ma'lumotlarni himoya qilish bilan birga tahdidlarni baholash metodologiyalari tartibga soluvchi talablarga mos kelishini ta'minlashi kerak.

Tahdidlarni baholash va prognoz qilish muhimligini ko‘rsatuvchi yorqin misol 2020-yil dekabr oyida kashf etilgan SolarWinds ta’minot zanjiri hujumidir. Bu murakkab kiberhujum butun dunyo bo‘ylab minglab tashkilotlarga, jumladan, davlat

[4] Ogcu Kaya, G., Demirel, O. F. Parameter Optimization of Intermittent Demand Forecasting by Using Spreadsheet. Kybernetes 2015. P.211.

ISSN 2181-3187

idoralari va tashkilotlarga zararli dasturlarni tarqatish uchun SolarWinds'ning Orion dasturiy ta'minoti yangilanishlarini buzishni o'z ichiga olgan[5].

2017 yilda WannaCry to'lov dasturi hujumi tahdidlarni noto'g'ri baholash va kamaytirish oqibatlarining yorqin namunasi bo'lib xizmat qiladi. Microsoft-ning Server Message Block (SMB) protokolidagi zaiflikdan foydalangan holda, WannaCry butun dunyo bo'ylab tarmoqlar bo'ylab tez tarqaldi, ma'lumotlarni shifrladi va Bitcoinda to'lovni talab qildi. Microsoft tomonidan bir necha oy oldin e'lon qilingan muhim xavfsizlik tuzatmasidan foydalana olmagan tashkilotlar hujum qurboni bo'lishdi, bu esa sog'liqni saqlash, hukumat va moliya sektorlarida keng tarqalgan buzilishlarga olib keldi. WannaCry hodisasi zaifliklarni o'z vaqtida boshqarish muhimligini va tashkilotlarning zararli shaxslar tomonidan ekspluatatsiya qilish xavfini kamaytirish uchun muhim zaifliklarni tuzatishga ustuvor ahamiyat berish zarurligini ta'kidladi.

Fishing eng keng tarqalgan kiber tahdidlardan biri bo'lib qolmoqda, u foydalanuvchilarni maxfiy ma'lumotlarni oshkor qilish yoki zararli qo'shimchalarni yuklab olishda aldash uchun ijtimoiy muhandislik taktikasiga tayanadi. Fishing hujumlari kontekstida tahdidni baholash fishing urinishlari ko'rsatkichlari uchun elektron pochta sarlavhalari, kontent va URL manzillarini tahlil qilishni o'z ichiga oladi. Mashinani o'rganish algoritmlari va elektron pochtani filtrlash echimlari fishing kampaniyalarini ko'rsatadigan shubhali naqshlar va anomaliyalarni aniqlash orqali aniqlash imkoniyatlarini oshiradi.

Axborot xavfsizligiga tahdidlarni bashorat qilish tashkilotlar tobora murakkab va doimiy kibertahdidlarga duch kelayotgan bugungi raqamli landshaftda muhim vazifa hisoblanadi. Ushbu dissertatsiya axborot xavfsizligiga tahdidlarni prognoz qilishning metodologiyalari, muammolari va real misollarini o'rganib, potentsial xavflarni yumshatishda proaktiv choralar muhimligini ta'kidlaydi.

Axborot xavfsizligiga tahdidlarni bashorat qilish potensial xavflarni bashorat qilish uchun tendensiyalar, rivojlanayotgan texnologiyalar, tahdidlar bo'yicha razvedka va tarixiy ma'lumotlarni tahlil qilishni o'z ichiga oladi. Asosiy metodologiyalarga quyidagilar kiradi:

1. Tahdid razvedkasi tahlili: turli manbalardan, jumladan, xavfsizlik tasmasi, qorong'u veb monitoringi va kiberxavfsizlik hisobotlaridan tahdidlar haqidagi ma'lumotlarni to'plash va tahlil qilish. Tahdid razvedkasi platformalari tahdid

[5] Neuhaus, S., Zimmermann, T., Holler, C., Zeller, A. Predicting Vulnerable Software Components. In: Ning, P. (Ed.), Proceedings of the Fourteenth ACM Conference on Computer and Communications Security. Association for Computing Machinery, October 29-November 2, Alexandria, Virginia, USA, pp. 2007. p.109.

ISSN 2181-3187

qiluvchilar tomonidan qo'llaniladigan yangi tahdidlar, taktikalar, usullar va protseduralarni (TTP) aniqlash uchun ma'lumotlarni jamlaydi va tahlil qiladi[6].

2. Trend tahlili: ransomware hujumlari, fishing kampaniyalari yoki muayyan dasturiy ta'minot va texnologiyalar bilan bog'liq zaifliklar kabi kiberxavfsizlik tendentsiyalarini kuzatish va tahlil qilish. Trend tahlili tashkilotlarga tarixiy naqshlar va sanoat rivojlanishi asosida potentsial tahdidlarni oldindan bilishga yordam beradi.

3. Ssenariyga asoslangan prognozlash: potentsial tahdid vektorlari, zaifliklar va tashkiliy xavf omillari asosida gipotetik stsenariylarni ishlab chiqish. Stsenariyga asoslangan prognozlash proaktiv rejalashtirish va kiberxavfsizlikning bir qator hodisalari va tahdid stsenariylariga tayyorgarlik ko'rish imkonini beradi.

Advanced Persistent Threats (APT) - bu odatda milliy davlat aktorlari yoki uyushgan kiberjinoyat guruhlari tomonidan uyushtirilgan murakkab kiberhujumlar. APTlar ko'pincha davlat idoralari, mudofaa pudratchilari va muhim infratuzilma tarmoqlaridagi tashkilotlarni nishonga oladi.

Prognozlash misoli: 2020-yilda kiberxavfsizlik bo‘yicha tadqiqotchilar COVID-19 pandemiyasi davrida sog‘liqni saqlash tashkilotlariga qaratilgan APT faolligi oshishini prognoz qilishdi. Tahdid aktorlari bemorlarning sirli ma’lumotlarini o‘g‘irlash va sog‘liqni saqlash xizmatlarini to‘xtatish uchun masofadan kirish vositalari va sog‘liqni saqlash IT tizimlaridagi zaifliklardan foydalangan.

Zeroday ekspluatatsiyalar sotuvchiga noma'lum bo'lgan va mavjud tuzatish yoki tuzatishga ega bo'lmagan dasturiy ta'minot yoki apparatdagi zaifliklarga ishora qiladi. Xavfsizlik guruhlari yumshatish choralarini ishlab chiqish va qo'llashdan oldin, tahdid aktyorlari maqsadli hujumlarni boshlash uchun nol kunlik zaifliklardan foydalanadi[7].

Xavfsizlik bo‘yicha tadqiqotchilar 2021-yilda mashhur veb-brauzerlarga mo‘ljallangan zeroday ekspluatatsiyalar ko‘payishini prognoz qilishdi. Tahdid qiluvchilar o‘zboshimchalik bilan kodni ishga tushirish, hisob ma’lumotlarini o‘g‘irlash va buzilgan veb-saytlar va fishing kampaniyalari orqali zararli dasturlarni tarqatish uchun brauzerning zaifliklaridan foydalangan.

Tahdidlar bo'yicha razvedka va prognozlash metodologiyasidagi yutuqlarga qaramay, kibertahdidlarni to'g'ri bashorat qilish va yumshatishda bir qator muammolar mavjud:

1. Tahdid landshaftining murakkabligi: kibertahdidlarning tez evolyutsiyasi, shu jumladan yangi hujum vektorlari va usullari tahdidlarni prognoz qilishni

[6] Kim, J., Malaiya, Y., Ray, I. Vulnerability Discovery in Multi-Version Software Systems. In: Cukic, B., Dong, J. (Eds.), Proceedings of the Tenth IEEE High Assurance Systems Engineering Symposium. IEEE Computer Society, November 14-16, Dallas, Texas, USA, 2007. P.73.

[7] Arora, A., Krishnan, R., Telang, R., Yang, Y. An Empirical Analysis of Software Vendors’ 670 Patch Release Behavior: Impact of Vulnerability Disclosure. Information Systems Research. 2010. P.142.

ISSN 2181-3187

murakkablashtiradi. Tahdid qiluvchilar aniqlanmaslik va paydo bo'lgan zaifliklardan foydalanish uchun o'z taktikalarini doimiy ravishda yangilaydi va moslashtiradi.

2. Ma'lumotlarning aniqligi va o'z vaqtidaligi: O'z vaqtida va to'g'ri tahdid razvedkasi ma'lumotlarini olish samarali prognoz qilish uchun juda muhimdir. Tahdid ma'lumotlaridagi kechikishlar yoki noaniqliklar tashkilotlarning paydo bo'layotgan tahdidlarga proaktiv javob berish qobiliyatiga to'sqinlik qilishi mumkin.

3. Insayder tahdidlar va inson omillari: Insayder tahdidlar, jumladan, beparvo yoki yomon niyatli xodimlar tahdidlarni prognoz qilishda jiddiy qiyinchiliklar tug‘diradi. Tashkilotlar xavfsizlik bo'yicha kuchli treningni o'tkazishi va ichki xavflarni kamaytirish uchun xodimlarning xatti-harakatlarini kuzatishi kerak.

Axborot xavfsizligi holatini tahlil qilish (yoki axborot tizimining xavfsizligini baholash) kompaniyalarga paydo bo'lgan tahdidlarni o'z vaqtida aniqlash va bartaraf etishga yordam beradigan tuzilgan, takrorlanadigan jarayondir. Tahlil natijalariga ko'ra kompaniyaning ichki jarayonlarini o'zgartirishga qaratilgan tavsiyalar shakllantiriladi. Xavfning yuzaga kelish ehtimoli va mumkin bo'lgan zarar darajasini aniqlash uchun tahlil qilish ham zarur.

Axborot xavfsizligini tahlil qilish xavfsizlik tizimi uni keyingi loyihalash, modernizatsiya qilish va zarur xavfsizlik choralarini amalga oshirish uchun qanday bo'lishi kerakligini tushunishga yordam beradi, bu esa, o'z navbatida, korxona ma'lumotlarini ruxsatsiz kirishdan himoya qilishning zarur darajasini ta'minlaydi. Xavfsizlikni tahlil qilishda foydalanish mumkin bo'lgan bir nechta turli xil metodologiyalar mavjud[8].

1. Ekspert bahosi. Ekspert komissiyasi tadqiqotga kiritiladigan ob'ektlarni, shuningdek ularning parametrlari va xususiyatlarini belgilaydi.

Korxonaning axborot xavfsizligi samaradorligini to'liq baholash uchun mutaxassislar quyidagi ma'lumotlarni yig'adilar:

- avtomatlashtirish ob'ekti haqida umumiy ma'lumot;
- maxfiy axborotni qayta ishlash jarayonlarining tavsifi;
- korporativ axborot tizimining tavsifi;
- axborot infratuzilmasining tavsifi;
- axborot xavfsizligi tizimining tavsifi (hujjatlar, tashkiliy-texnik tadbirlar, himoya vositalari).

Yig'ilgan ma'lumotlarga asoslanib, mutaxassislar potentsial xavf manbalarini baholaydilar. Har bir aniqlangan manba uchun tahdidning yuzaga kelish ehtimoli va muhimlik koeffitsienti aniqlanadi.

[8] Alhazmi, O., Malaiya, Y., Ray, I. Security Vulnerabilities in Software Systems: A Quantitative Perspective. In: Jajodia, S., Wijesekera, D. (Eds.), Proceedings of the 19th Annual IFIP 660 WG 11.3 Working Conference on Data and Applications Security. Vol. 3654 of Lecture Notes in Computer Science. Springer-Verlag, Berlin, Heidelberg, August 7-10, Storrs, Connecticut, USA. 2005. P.93.

ISSN 2181-3187

2. Xatarlarni statistik tahlil qilish. Ushbu usul tizimning eng zaif joyini aniqlash imkonini beradi. Biroq, bunday tahlil qilish uchun avval sodir etilgan hujumlar haqida etarlicha katta hajmdagi ma'lumotlarga ega bo'lish kerak.

3. Faktor tahlili. IT mutaxassislari ma'lum bir tahdidning paydo bo'lishiga sifat jihatidan ta'sir qiluvchi asosiy omillarni aniqlaydilar. Mutaxassisning vazifasi korxona tizimlarini tahlil qilish va qaysi zaifliklarni bartaraf etish va qaysi birini e'tiborsiz qoldirish mumkinligini aniqlashdir.

Axborot xavfsizligi holatini tahlil qilish doirasida mutaxassis hujum vektorlarini yoki potentsial tajovuzkor tizimga zarar etkazishi mumkin bo'lgan vositalarni ham aniqlaydi.

Ba'zi tahdidlarga misollar:

- foydalanuvchilarning fishing hujumlariga tayyor emasligi;
- himoyalanmagan simsiz tarmoqlardan foydalanish;
- ochiq USB portlari va olinadigan muhitdan nazoratsiz foydalanish imkoniyati;
- komponentlarning eskirgan versiyalarining mavjudligi

Korxonaning axborot xavfsizligini baholash doimiy, doimiy, davriy hodisaga aylanishi kerakligini tushunish muhimdir. Har kuni xakerlar ma'lumotlarni o'g'irlashning yangi usullari va usullarini o'ylab topadilar va yangi zaifliklar paydo bo'ladi.

Tizim xavfsizligi tahlili quyidagi hollarda ayniqsa dolzarb bo'ladi:

- tanqidiy vaziyatlar;
- kompaniyaning qo'shilishi, qo'shilishi, qo'shilishi, kengayishi;
- kurs yoki biznes kontseptsiyasini o'zgartirish;
- qonun hujjatlaridagi o'zgarishlar;
- axborot tuzilmasidagi katta o'zgarishlar.

Axborot xavfsizligini baholash jarayoni biznesdan biznesga farq qilishi mumkin. Biroq, asosiy baholash bosqichlari takrorlanishi, sanoatning ilg'or tajribalariga asoslangan bo'lishi va tizimlarning to'liq hajmini va ularning potentsial zaifliklarini baholashni ta'minlash uchun tuzilgan bo'lishi kerak.

Quyida mumkin bo'lgan tahdidlarni baholash uchun ishlatiladigan bir nechta mavjud usullar mavjud.

Axborot oqimini modellashtirish yordamida axborot xavfsizligini baholash jarayoni quyidagilarni aniqlaydi:

- tizim xatti-harakatlaridagi tendentsiyalar;
- mumkin bo'lgan xatolarning paydo bo'lishi;
- zaifliklar ko'lami;
- ehtimoliy tahdidning oqibatlari ko'lami.

ISSN 2181-3187

Butun tizimni dastlabki baholash va potentsial xavflarni aniqlash xavfsizlik choralari bo'yicha samarali qaror qabul qilish imkonini beradi.

Foydalanilgan adabiyotlar:

1. Ozment, A., 2006. Software Security Growth Modeling: Examining Vulnerabilities with Reliability Growth Models. In: Gollmann, D., Massacci, F., Yautsiukhin, A. (Eds.), Proceedings of the First Workshop on Quality of Protection. Vol. 23 of Advances in Information Security. Springer Boston 790 Massachusetts, September 19-22, Como, Italy, pp. 1–13

2. R.C. Fong and A. Vedaldi. 2017. Interpretable Explanations of Black Boxes by Meaningful Perturbation. In Proceedings of the 16th International Conference on Computer Vision (ICCV).

3. Roumani, Y., Nwankpa, J. K., Roumani, Y. F., 2015. Time Series Modeling of Vulnerabilities. Computers & Security 51, 32–40.