VOLUME-1, ISSUE-12

Kiberxavfsizlik tushunchalari va asoslari

Tursunov Davronbek Baxodir o'g'li

Toshkent davlat yuridik universiteti magistratura bosqichining "Kiber huquqi" mutaxassisligi talabasi

Annotatsiya: Ushbu maqolaning maqsadi kiberxavfsizlikning asosiy tushunchalariga ta'rif bergan holda, uning huquqiy tomonlarini ochib berish.

Kalit so'zlar: Kiberxavfsizlik, kiberhujum, signal

Kiberxavfsizlikning ta'rifi bu apparat, dasturiy ta'minot va ma'lumotlar kabi Internetga ulangan tizimlarni kiber tahdidlardan himoya qilish ekanligini tushunishdir. Ushbu amaliyot jismoniy shaxslar va korxonalar tomonidan ma'lumotlar markazlari va boshqa kompyuterlashtirilgan tizimlarga ruxsatsiz kirishdan himoya qilish uchun qo'llaniladi. Kuchli kiberxavfsizlik strategiyasi tashkilot yoki foydalanuvchi tizimlari va maxfiy ma'lumotlariga kirish, o'zgartirish, yo'q qilish, yo'q qilish yoki tovlamachilikka qaratilgan zararli hujumlardan yaxshi himoyani ta'minlashi mumkin. Kiberxavfsizlik tizim yoki qurilmani o'chirish yoki buzishga qaratilgan hujumlarning oldini olishda ham muhim rol o'ynaydi.

Kiberxavfsizlikning afzalligi zamonaviy korxonada foydalanuvchilar, qurilmalar va dasturlar sonining ortib borishi, shuningdek, ko'p qismi maxfiy yoki maxfiy bo'lgan ma'lumotlar oqimining ortib borishi bilan kiberxavfsizlikning ahamiyati o'sishda davom etmoqda. Kiberhujumlar va hujum usullari sonining ortib borayotgani va murakkabligi muammoni yanada kuchaytirmoqda.

Usbu maqolada kiberxavfsizlik qanday elementlardan iboratligi ko'rib chiqamiz. Kiberxavfsizlik sohasini bir nechta turli bo'limlarga bo'lish mumkin, ularni tashkilot ichida muvofiqlashtirish kiberxavfsizlik dasturining muvaffaqiyati uchun juda muhimdir. Ushbu bo'limlar quyidagilarni o'z ichiga oladi: axborot xavfsizligi yoki ma'lumotlar xavfsizligi; tarmoq xavfsizligi; favqulodda vaziyatlarni tiklash bo'yicha biznesning uzluksizligini rejalashtirish; muhim infratuzilma xavfsizligi; jismoniy xavfsizlik. Doimiy o'zgaruvchan tahdidlar landshaftida kiberxavfsizlikni

saqlab qolish barcha tashkilotlar uchun qiyinchilik tug'diradi. Doimiy o'zgaruvchan tahdidlar landshaftida kiberxavfsizlikni saqlab qolish barcha tashkilotlar uchun qiyinchilik tug'diradi. An'anaviy reaktiv yondashuvlar, bunda resurslar tizimlarni eng katta ma'lum bo'lgan tahdidlardan himoya qilishga yo'naltirilgan, kamroq ma'lum bo'lgan tahdidlar esa himoyasiz qolgan, endi etarli taktika emas. O'zgaruvchan xavfsizlik xavf-xatarlari bilan hamqadam bo'lish yanada faol va moslashuvchan yondashuvni talab qiladi. Kiberxavfsizlik bo'yicha bir nechta asosiy maslahat tashkilotlari ko'rsatmalar beradi.

Kiberxavfsizlik amaliyotlarini joriy etish va qo'llab-quvvatlashning afzalliklari quyidagilardan iborat: biznesingizni kiberhujumlardan va ma'lumotlar sizib chiqishidan himoya qilish; ma'lumotlar va tarmoqlarni himoya qilish; ruxsatsiz foydalanuvchi kirishining oldini olish; buzg'unchilikdan keyin tiklanish vaqti qisqardi.

Shu qatorda kiberxavfsizlikning afzalliklardan tashqari uni joriy etishda bir necha muammolar mavjud bulardan biri, kiberxavfsizlik doimo xakerlar, ma'lumotlarning yo'qolishi, maxfiylik, xavflarni boshqarish va kiberxavfsizlik strategiyalarini o'zgartirish tahdidi ostida. Yaqin kelajakda kiberhujumlar soni kamayishi kutilmayapti. Doimiy ravishda hal qilinishi kerak bo'lgan asosiy muammolar qatoriga rivojlanayotgan tahdidlar, ma'lumotlar oqimi, kiberxavfsizlik bo'yicha treninglar, ishchi kuchi va malaka etishmasligi, ta'minot zanjiri va uchinchi tomon xavflari kiradi.

Kiberxavfsizlikning eng muammoli elementlaridan biri bu xavfsizlik xavflarining o'zgaruvchan tabiatidir. Yangi texnologiyalar paydo bo'lishi va yangi yoki turli usullarda qo'llanilishi bilan yangi hujum vektorlari ishlab chiqiladi. Hujumlardagi tez-tez sodir bo'ladigan o'zgarishlar va avanslarni kuzatib borish va ularga qarshi himoyani yangilash qiyin bo'lishi mumkin. Qiyinchiliklar potentsial zaifliklardan himoya qilish uchun barcha kiberxavfsizlik elementlarini yangilab turishini ta'minlashni o'z ichiga oladi. Bu ayniqsa, etarli xodimlar yoki o'z resurslariga ega bo'lmagan kichik tashkilotlar uchun qiyin bo'lishi mumkin. Bundan tashqari, tashkilotlar bir yoki bir nechta xizmatlaridan foydalanadigan odamlar haqida juda ko'p potentsial ma'lumotlarni to'plashi mumkin. Ko'proq ma'lumotlar to'planganligi sababli, yana bir tashvish - bu kiberjinoyatchi shaxsni aniqlash mumkin bo'lgan ma'lumotlarni o'g'irlashni xohlashi ehtimoli. Masalan, shaxsiy ma'lumotlarni bulutda

saqlaydigan tashkilot to'lov dasturi tomonidan hujumga uchrashi mumkin. Tashkilotlar bulutni buzishning oldini olish uchun hamma narsani qilishlari kerak. Kiberxavfsizlik dasturlari, shuningdek, oxirgi foydalanuvchi ta'limiga ham e'tibor qaratishi kerak. Xodimlar tasodifan ish joyiga noutbuklari yoki mobil qurilmalaridan tahdid va zaifliklarni olib kirishlari mumkin. Ular shuningdek, havolalarni bosish yoki fishing elektron pochtalaridan qo'shimchalarni yuklab olish kabi xavfli harakat qilishlari mumkin. Doimiy xavfsizlik bo'yicha treninglar xodimlarga o'z kompaniyasini kiber tahdidlardan himoya qilishda yordam beradi. Kiberxavfsizlikning yana bir muammosi - kiberxavfsizlik bo'yicha malakali xodimlarning etishmasligi. Korxonalar tomonidan to'plangan va foydalaniladigan ma'lumotlar hajmi oshgani sayin, kiberxavfsizlik bo'yicha mutaxassislarga hodisalarni tahlil qilish, boshqarish va ularga javob berishga bo'lgan ehtiyoj ham ortib bormoqda. Tadqiqotlarga ko’ra? Dunyo bo’ylab kerakli kiberxavfsizlik ishlari va xavfsizlik mutaxassislari o'rtasidagi tafovutni 3,4 millionga baholadi. Tashkilotlar xavfsizlikni ta'minlash uchun qo'lidan kelgan barcha ishni qilishlari mumkin, ammo agar hamkorlar, sotuvchilar va ularning tarmoqlariga kirish huquqiga ega bo'lgan uchinchi tomon provayderlari xavfsiz harakat qilmasa, bu harakatlar behuda bo'ladi. Ta'minot zanjiri dasturiy ta'minoti va apparat hujumlari tobora qiyinlashib borayotgan xavfsizlik muammosidir. Tashkilotlar ta'minot zanjiridagi uchinchi tomon risklarini bartaraf etishlari va dasturiy ta'minotni ta'minlash bilan bog'liq muammolarni kamaytirishlari kerak, masalan, dasturiy ta'minot spetsifikatsiyalaridan foydalanishi lozimdir.

Shunday qilib, axborot xavfsizligini ta'minlashning asosiy vazifasi zaifliklarni, axborot xavfsizligiga potentsial va real tahdidlarni aniqlash va ta'sirini minimallashtirishdan iborat. Xavfli signallarning yo'qligi yuz foiz himoyani anglatmaydi. Biroq, muammolar aniqlanganda imkon qadar tez va samarali harakat qilishga intilish kerak. Tashqi va ichki muhitning zamonaviy sharoitlari axborot xavfsizligini ta'minlashda sifat jihatidan yangi samarali yondashuvlarni talab qilmoqda.

Manbaalar:

1. https://lex.uz/uz/docs/5960604 ;

2. Libicki M. What is information warfare? - http://www. ndu.edu/, 15.07.04г; Schwartau W. An Introduction to Information Warfare // War in the information Age. New Challenges for US Security Policy. - Washington etc., 1997; Stein G. Information War - Cyberwar - Netwar // http:// www.infowar.com/mil_34i/stein1 .html-ssi, 21/05.04;

3. Information technology — Vocabulary: knowledge concerning objects, such as facts, events, things, processes, or ideas, including concepts, that within a certain context has a particular meaning. ISO/IEC 2382:2015;

4. Galitsky B. Polls «Internet in Russia». 2002 [Electronic resource]. 2002. www.fom.ru/ reports/frames/body/o0209241.html (date of appeal: 2020)