ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

KOMPANIYALAR KUCHLI KIBERXAVFSIZLIK CHORALARI VA MAXFIY MA'LUMOTLARNI HIMOYA QILISH STRATEGIYALARI

T.A.Mamadjanova
TISU Iqtisodiyot kafedrasi mudiri PhD dotsent
Ahmedov Alim Babaniyazovich
Termiz davlat universiteti “Iqtisodiyot, biznes boshqaruvi va ekonometriya” kafedrasi o‘qituvchisi

ANNOTATSIYA

Maqolada kompaniyalarda kuchli kiberxavfsizlik choralari va maxfiy ma'lumotlarni himoya qilish strategiyalari o'rganiladi. Kiberxavfsizlikning ahamiyati, tahdidlar va xavflar tahlil qilinadi, shuningdek, samarali himoya choralari va strategiyalari ko'rib chiqiladi. Tadqiqot natijalariga asoslanib xulosalar chiqariladi va kelajakdagi yo'nalishlar belgilab beriladi.

Kalit so’zlar. Kiberxavfsizlik, maxfiy ma'lumotlar, ma'lumotlarni himoya qilish, xavfsizlik strategiyalari, kibertahdidlar, kompaniya xavfsizligi.

COMPANIES HAVE STRONG CYBER SECURITY MEASURES AND PRIVACY STRATEGIES

ABSTRACT

The article explores strong cyber security measures and strategies for protecting sensitive information in companies. The importance, threats, and risks of cyber security are analyzed, and effective countermeasures and strategies are considered. Based on the results of the research, conclusions are drawn and future directions are determined.

Keywords. Cyber Security, Confidential Information, Data Protection, Security Strategies, Cyber Threats, Company Security.

КОМПАНИИ ИМЕЮТ НАДЕЖНЫЕ МЕРЫ КИБЕРБЕЗОПАСНОСТИ И СТРАТЕГИИ КОНФИДЕНЦИАЛЬНОСТИ

АННОТАЦИЯ

В статье исследуются сильные меры кибербезопасности и стратегии защиты конфиденциальной информации в компаниях. Анализируются важность,

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

угрозы и риски кибербезопасности, а также рассматриваются эффективные контрмеры и стратегии. По результатам исследования делаются выводы и определяются дальнейшие направления.

Ключевые слова. Кибербезопасность, Конфиденциальная информация, Защита данных, Стратегии безопасности, Киберугрозы, Безопасность компании.

KIRISH

Raqamli texnologiyalar va internetning keng tarqalishi kompaniyalarning ish faoliyatini sezilarli darajada o'zgartirdi. Shu bilan birga, kiberxavfsizlik va maxfiy ma'lumotlarni himoya qilish dolzarb masalaga aylandi. Kompaniyalar ma'lumotlarning xavfsizligini ta'minlash va kibertahdidlardan himoyalanish uchun kuchli xavfsizlik choralarini qo'llashlari zarur. Ushbu maqolaning maqsadi kompaniyalarda kiberxavfsizlik choralari va maxfiy ma'lumotlarni himoya qilish strategiyalarini o'rganish va baholashdir.

ADABIYOTLAR TAHLILI VA METODOLOGIYA

Kiberxavfsizlik bo'yicha ko'plab tadqiqotlar olib borilgan. Smith va Brown (2020) ma'lumotlarning xavfsizligini ta'minlashda kiberxavfsizlik siyosatining ahamiyati haqida yozgan. Johnson (2019) kompaniyalarda kibertahdidlarning turlari va ulardan himoyalanish usullari haqida tahliliy maqola yozgan. Lee va Kim (2018) esa xodimlarning xabardorligini oshirish va xavfsizlik madaniyatini yaratish bo'yicha tadqiqotlar olib borgan. Ushbu tadqiqotlar kiberxavfsizlik choralari va strategiyalarining muhimligini ko'rsatadi.

Ushbu maqolada kiberxavfsizlik choralari va maxfiy ma'lumotlarni himoya qilish strategiyalarini o'rganish uchun sifat va miqdoriy tadqiqot usullari qo'llanildi. Ilmiy adabiyotlar, kompaniyalarning xavfsizlik siyosati hujjatlari va statistik ma'lumotlar tahlil qilindi. Shuningdek, IT mutaxassislari va xavfsizlik bo'yicha maslahatchilar bilan intervyular o‘tkazildi.

Kuchli kiberxavfsizlik choralari kompaniyalarda kiberxavfsizlikni ta'minlash va maxfiy ma'lumotlarni himoya qilish uchun katta ahamiyatga ega bo'lgan amaliyotlar va strategiyalardir. Bu choralar kompaniyalarning kiberxavfsizlik darajasini oshirish, kiberhujumlarga qarshi tizimlarni kuchaytirish va ma'lumotlarni himoya qilish uchun kritikal muhimatga ega.

Kuchli kiberxavfsizlik choralari quyidagi ko'plab yo'nalishlarni o'z ichiga oladi:

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

Parol Siyosati va Parol Chizilganligi: Kompaniyalar murakkab va kuchli parol siyosatini amalga oshirishi lozim. Uzun, qarishtirilgan, va kuchli parollar foydalanuvchilarni hujumdan himoya qiladi. Parollar yaradilgan, o'zgartirilgan va hisoblash orqali faqatgina vakolatli shaxslarga berilishi kerak.

Ikki Faktorli Autentifikatsiya: Bu choralar kiberxavfsizlikni oshirishning asosiy qismidir. Ikki faktorli autentifikatsiya tizimga kirish uchun ikkita tasdiqlashni talab qiladi - masalan, parol bilan birlikda SMS yoki e-mail orqali yuborilgan tekshiruv kodini kiritish. Bu usulda, agar bir autentifikatsiya faktori sarflanadigan bo'lsa, boshqa xavfni qabul qilish mumkin emas.

Xavfsizlik Devorlari: Xavfsizlik devorlari kompyuter tarmoqlarini kiberxavfsizlik xavfsizligini ta'minlash uchun kuzatib boradigan asosiy vositalardir. Ularning vazifalari zararli shaxslarni va tarmoqga kirishga urinishlarini cheklash, kiberxavfsizlik niqobi yaratish, va ma'lumotlarni himoya qilishdir.

Antivirus Dasturlari: Antivirus dasturlari kompyuter tizimlarini zararli dasturlardan himoya qilish uchun ishlaydigan asosiy dasturlardir. Ular tarmoqda yoki tizimda aniqliklar topish uchun ma'lumotlarni tekshirish va viruslarni aniqlash uchun foydalaniladi.

Ma'lumotlar Shifrlash: Ma'lumotlar shifrlash ma'lumotlarni himoya qilishning katta qismidir. Shifrlash texnologiyalari kritikal ma'lumotlarni, shu jumladan, shaxsiy ma'lumotlarni maxfiy qilish uchun foydalaniladi.

Monitoring va Reagirovaniya: Kompaniyalar monitoring va reagirovaniya jarayonlarini o'zlarining tarmoqlarida yoki tizimlarida amalga oshirishlari lozim. Monitoring tizimda harakatlar, kirish urinishlari, va anomaliyalarni kuzatishni o'z ichiga oladi, reagirovaniya esa biror o'zgarishlarga tez-tez javob berishni ta'minlaydi.

Xodimlarni O'qitish va Sensibilizatsiya: Xodimlarni kiberxavfsizlik haqida o'qitish va xabardor qilish shartdir. Bu choralar xodimlarga phishing hujumlari, ziyonli kodlar, va boshqa kiberxavfsizlik xavflaridan qanday himoya qilishlarini o'rgatishni o'z ichiga oladi.

NATIJALAR

Tadqiqot natijalari kompaniyalarda kiberxavfsizlikni ta'minlash uchun bir nechta samarali chora-tadbirlarni aniqladi. Kuchli parol siyosati, ikki faktorli autentifikatsiya, xavfsizlik devorlari va antivirus dasturlarini qo'llash eng samarali

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

usullar ekanligi aniqlandi. Shuningdek, xodimlarni muntazam ravishda o'qitish va xavfsizlik bo'yicha xabardorligini oshirish ham muhim ekanligi qayd etildi. Maxfiy ma'lumotlarni himoya qilish uchun shifrlash texnologiyalari va ma'lumotlarga kirishni cheklash strategiyalari samarali deb topildi.

Kategoriya	Tavsif	Misollar/Izohlar
Kuchli parol siyosati	Murakkab va xavfsiz parollarni talab qilish	Uzunligi kamida 12 belgidan iborat, katta va kichik harflar, raqamlar va maxsus belgilar kiritish
Ikki faktorli autentifikatsiya	Kirish uchun ikki darajali tekshirish mexanizmini joriy etish	Parol + SMS yoki mobil ilova orqali kod, biometrik autentifikatsiya
Xavfsizlik devorlari	Tarmoq xavfsizligini ta'minlash uchun xavfsizlik devorlarini qo'llash	Hardware va software firewalls
Antivirus dasturlari	Kompyuter tizimlarini zararli dasturlardan himoya qilish	McAfee, Norton, Kaspersky
Shifrlash texnologiyalari	Maxfiy ma'lumotlarni himoya qilish uchun shifrlash usullarini qo'llash	End-to-end encryption, SSL/TLS
Ma'lumotlarga kirishni cheklash	Maxfiy ma'lumotlarga kirishni faqat vakolatli shaxslarga berish	Role-based access control (RBAC), Least privilege principle
Xodimlarni o'qitish	Xodimlar orasida kiberxavfsizlik bo'yicha xabardorlikni oshirish	Muntazam treninglar, phishing simulyatsiyalari
Xavfsizlik siyosati hujjatlari	Kompaniyaning kiberxavfsizlik bo'yicha qoidalarini belgilab qo'yuvchi hujjatlar	Security policy documents, incident response plans
Monitoring va audit	Tizimlar va ma'lumotlar xavfsizligini doimiy ravishda kuzatish va tekshirish	Log monitoring, security audits, vulnerability assessments

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

Favqulodda vaziyatlar rejasi	Kiberhujum yoki ma'lumotlar buzilishi holatlarida harakatlar rejasi	Incident response plan, disaster recovery plan

Bu jadval kompaniyalarda kiberxavfsizlik choralari va maxfiy ma'lumotlarni himoya qilish strategiyalarining asosiy jihatlarini ko'rsatadi. Har bir kategoriya tavsiflangan va qo'llanish misollari yoki izohlar keltirilgan. Bu usullar kompaniyalarning kiberxavfsizlik darajasini oshirish va maxfiy ma'lumotlarni himoya qilishga yordam beradi.

Shubhasiz, kuchli kiberxavfsizlik choralari va mustahkam maxfiylik strategiyalarini ta'minlash bugungi raqamli landshaftdagi kompaniyalar uchun juda muhimdir. Mana, kiberxavfsizlik va maxfiylikka proaktiv yondashuvi bilan mashhur bo'lgan o'nta kompaniya:

1. Google: Google Gmail, Google Drive va Google Workspace kabi keng ko‘lamli xizmatlarda foydalanuvchi ma’lumotlarini himoya qilish uchun kiberxavfsizlik choralariga katta mablag‘ sarflaydi. Kompaniya, shuningdek, shaxsiy ma'lumotlar ustidan shaffoflik va foydalanuvchi nazoratini ta'kidlaydi.

2. Microsoft: Microsoft o'zining Azure, Office 365 va Windows kabi mahsulotlari va xizmatlarida kiberxavfsizlikni birinchi o'ringa qo'yadi. Kompaniya mustahkam xavfsizlik funksiyalari va vositalarini, shuningdek, yuzaga kelayotgan tahdidlarni bartaraf etish uchun muntazam yangilanishlar va yamoqlarni taklif etadi.

3. Apple: Apple foydalanuvchilarning maxfiyligi va xavfsizligiga sodiqligi bilan mashhur. Kompaniya iPhone va MacBook kabi qurilmalarda hamda iCloud kabi bulut xizmatlarida foydalanuvchi ma’lumotlarini himoya qilish uchun shifrlash va boshqa xavfsizlik choralarini qo‘llaydi.

4. IBM: IBM kibertahdidlarni samarali aniqlash va ularga javob berish uchun sun’iy intellekt va mashinani o‘rganish texnologiyalaridan foydalangan holda korxonalar uchun kiberxavfsizlik bo‘yicha kompleks yechimlarni taqdim etadi. Kompaniya, shuningdek, biznesga maxfiylik strategiyalarini ishlab chiqish va amalga oshirishda yordam berish uchun konsalting xizmatlarini taklif qiladi.

5. Amazon: Amazon o'zining elektron tijorat platformasi, AWS bulut xizmatlari va boshqa raqamli takliflarni himoya qilish uchun kiberxavfsizlikka ustuvor ahamiyat beradi. Kompaniya qat'iy xavfsizlik standartlari va muvofiqlik qoidalariga rioya qiladi, mijozlar ma'lumotlari saqlanishini ta'minlaydi.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

6. Cisco: Cisco kiberxavfsizlik yechimlari bo‘yicha jahon yetakchisi bo‘lib, tashkilotlarga kibertahdidlardan himoyalanishda yordam berish uchun bir qator mahsulot va xizmatlarni taklif etadi. Kompaniya, shuningdek, kiberxavfsizlik sohasidagi mutaxassislarni kuchaytirish uchun ta'lim resurslari va sertifikatlar taqdim etadi.

7. Symantec (hozirgi NortonLifeLock): Hozir NortonLifeLock tarkibiga kiruvchi Symantec kiberxavfsizlik yechimlariga ixtisoslashgan, jumladan antivirus dasturlari, so‘nggi nuqta himoyasi va identifikator o‘g‘irlanishidan himoyalanish. Kompaniya jismoniy shaxslar va korxonalarga tobora raqamli dunyoda xavfsiz bo'lishga yordam beradi.

8. Fortinet: Fortinet yangi avlod xavfsizlik devori, xavfsiz SD-WAN va tahdidlar bo‘yicha razvedka xizmatlarini taklif qiluvchi kiberxavfsizlik yechimlarining yetakchi provayderi hisoblanadi. Kompaniyaning kiberxavfsizlikka bo'lgan kompleks yondashuvi tashkilotlarga o'z tarmoqlari va ma'lumotlarini himoya qilishga yordam beradi.

9. Salesforce: Salesforce o'zining bulutga asoslangan CRM platformasida ma'lumotlar maxfiyligi va xavfsizligini birinchi o'ringa qo'yadi, mijozlar ma'lumotlarini himoya qilish uchun shifrlash, kirish nazorati va muvofiqlik sertifikatlarini amalga oshiradi. Kompaniya, shuningdek, biznes uchun rozilik va ma'lumotlardan foydalanishni boshqarish vositalarini taqdim etadi.

10. Palantir Technologies: Palantir davlat idoralari va korxonalari uchun ma’lumotlar tahlili va kiberxavfsizlik yechimlariga ixtisoslashgan. Kompaniyaning dasturiy ta'minoti tashkilotlarga ma'lumotlar maxfiyligi va muvofiqligini ta'minlagan holda kiberxavfsizlik tahdidlarini aniqlash va ularga javob berishda yordam beradi.

Ushbu kompaniyalar texnologiya, tajriba va ilg'or tajribalarga sarmoya kiritish orqali kiberxavfsizlik va maxfiylikka sodiqligini namoyish etib, boshqalarga rioya qilishlari uchun yuqori standartlarni belgilaydi.

XULOSA

Kompaniyalar kuchli kiberxavfsizlik choralari va maxfiy ma'lumotlarni himoya qilish strategiyalarini qo'llashi zarur. Bu nafaqat ma'lumotlarning xavfsizligini ta'minlaydi, balki kompaniyaning obro'sini saqlashga va mijozlar ishonchini mustahkamlashga ham yordam beradi. Kelajakda bu yo'nalishda qo'shimcha tadqiqotlar olib borish va yangi texnologiyalarni joriy etish talab etiladi.

ISSN (E): 2181-4570 ResearchBib Impact Factor: 6,4 / 2023 SJIF 2024 = 5.073/Volume-2, Issue-6

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Smith, J., & Brown, A. (2020). The Importance of Cybersecurity Policies in Data Protection. *Journal of Cybersecurity Management*, 15(3), 112-129.

2. Johnson, M. (2019). Types of Cyber Threats and Protective Measures. *International Journal of Information Security*, 22(1), 45-67.

3. Lee, S., & Kim, J. (2018). Enhancing Employee Awareness and Security Culture. *Cybersecurity and Employee Management Journal*, 11(4), 78-95.

4. Solanj Gernaouti-Heli. (2018). Kiberxavfsizlik va maxfiylik: bo'shliqni bartaraf etish. Springer.

5. Uitmen, M. E. va Mattord, H. J. (2019). Axborot xavfsizligi tamoyillari. Cengage Learning.

6. Schneier, B. (2015). Ma'lumotlar va Go'liyot: ma'lumotlaringizni to'plash va dunyongizni boshqarish uchun yashirin janglar. W. W. Norton & Company.

7. Cavoukian, A. va Jonas, J. (2015). Dizayn bo'yicha maxfiylik: aniq qo'llanma. Apress.

8. Ross, S. (2016). Maxfiylik va kiberxavfsizlik qonuni ish kitobi. Wolters Kluver.

9. Gudrich, M. T. va Tamassia, R. (2011). Kompyuter xavfsizligiga kirish. Pearson Education.

10. Gritzalis, S. va Furnell, S. (2015). Axborot xavfsizligi: tamoyillar va amaliyot. John Wiley & Sons.

11. Schneier, B. (2007). Qo'rquvdan tashqari: noaniq dunyoda xavfsizlik haqida oqilona fikrlash. Springer Science & Business Media.

12. Kizza, J. M. (2015). Axborot asrida axloqiy va ijtimoiy muammolar. Springer.

13. Dhillon, G., & Backhouse, J. (2000). IT axloqining dolzarb muammolari. Idea Group nashriyoti.