VEB-INTERFEYSDAN FOYDALANGAN XOLDA, MASOFAVIY BILIMNI BAXOLASH TIZIMLARIDA, MASOFAVIY MA'MURLASH XAVFSIZLIGINI TA'MINLASH

https://doi.org/10.5281/zenodo.10969942

Ochilov Nizomiddin Najmiddin o'g'li
O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Bilim va malakalarni baholash agentligi Axborot-kommunikatsiya texnologiyalarini joriy etish va raqamlashtirish boshqarmasi boshlig'i.
Abduxalimov Abdullaziz Komiljon o'g'li
O'zbekiston Respublikasi Oliy ta'lim, fan va innovatsiyalar vazirligi huzuridagi Bilim va malakalarni baholash agentligi Raqamli texnologiyalar bo'limi yetakchi mutaxassisi.

Annotatsiya: *Axborot texnologiyalarining inson faoliyatining barcha sohalariga joriy etilishi oliy kasbiy ta'lim sohasida yuqori malakali kadrlarni tayyorlashning zamonaviy shakllaridan foydalanish zaruriyatini taqazo etadi. Ushbu shakllar turiga bilimni masofadan baholash tizimlari kiradi. So'nggi yillarda masofaviy bilimni baholash tizimlari aytarli darajada rivojlandi. Ushbu tizimlar nazariy axborotni operativ tarzda olishga, talabgorni bilimini bir necha kilometr uzoqdan baholashga imkon beradi. Hozirgi kunda talabgorning haqiqiylikka tekshirish, bilimini haqqoniy aniqlash va uning shahsiy ma'lumotlarini xavfsizligini ta'minlash dolzarb hisoblanadi.*

Kalit so'zlar: *xavfsizlik, veb server, tahdid, zaiflik, risk.*

KIRISH

So'nggii yillarda masofaviy bilimni baholash tizimlari aytarli darajada rivojlandi. Ushbu tizimlar nazariy axborotni operativ tarzda olishga, talabgorni bilimini bir necha kilometr uzoqdan baholashga imkon beradi. Hozirgi kunda talabgorning haqiqiylikka tekshirish, bilimini haqqoniy aniqlash va uning shahsiy ma'lumotlarini xavfsizligini ta'minlash dolzarb hisoblanadi.

ASOSIY QISM

Zamonaviy ilovalarning aksariyati masofaviy ma'murlash funksiyalariga ega va uning xavfsizligi muhim xisoblanadi. Mobodo xaker ma'muriy sozlamalar ma'nosiga tushunib ulgursa, axborot xavfsizligini ta'minlash bo'yicha boshqa choralar foydasiz bo'lib qoladi.

Ma'sofaviy ma'murlash zaruriyatini quyidagi sabablarga ko'ra paydo bo'lishi mumkin:

•ko'chirilgan serverlar. Ma'mur har qanday ko'chirilgan veb-serverni (kompaniyaga tegishli, ammo internet-provayder hududida joylashgan kompyuterni) ma'murlash uchun interfeysga ehtiyoj sezadi;

•tashqi resurslarni jalb qilish. Xavfsizlik vositalari bilan ishlash keng ko'lamli bilimlarni talab etadi. Aksariyat kompaniyalar bunday bilimlarga ega emas. Shu sababli, kompaniyalar

xavfsizlik bo‘yicha barcha masalalarni ko‘pincha ushbu soha bo‘yicha ixtisoslashgan firmalar zimmasiga yuklaydi.

•fizik masofa. Yirik kompaniyaning ma’muri katta sonli kompyuterlarni boshqarishi mumkin. Ba’zi firmalar bir necha binolarda (shaharlarda) joylashganligi sababli, kompyuterlarga fizik xizmat ko‘rsatish zerikarli va ko‘p vaqt jalb etuvchi jalb etuvchi masalaga aylanadi.

Ilovani yoki kompyuterni masofadan ma’murlash uchun veb-interfeysdan foydalanishning quyidagi afzalliklarini ko‘rsatish mumkin:

•interfeys yaratilishining tezligi. Veb-interfeysning yaratilishi, grafik interfeysli mijozning yaratilishiga nisbatan kam vaqt sarfini talab etadi;

•operatsion tizimlarni madadlashi. Veb-serverdan foydalanish brauzer orqali barcha asosiy operatsion tizimlardan amalga oshirilishi mumkin (agar ishlab chiqaruvchilar Windows muhitida ishlovchi Activex kabi texnologiyadan foydalanmagan bo‘lsalar);

•foydalanuvchanlik. Veb-interfeysdan Internetdagi har qanday joydan foydalanish mumkin. Xatto, ofisda bo‘lmay turib ma’murlash amalga oshirilishi mumkin.

•foydalanuvchini o‘rgatish osonligi. Tizim ma’murining brauzer bilan muloqot qila olishi faraz qilinsa, uni o‘rgatishga kam vaqt sarf etiladi.

•foydalanuvchanlik. Veb-interfeysdan Internetdagi har qanday joydan foydalanish mumkinligi sababli, xakerni buzib kirishga intilishi mumkin;

•brauzer tomonidan boshqarish. Interfeys brauzer boshqaruvi ostida bo‘lganligi sababli, xakerga ma’murlash uchun grafik interfeysli alohida boshqaruvchi dasturni ishlatish kerak emas.

Ta’kidlash lozimki, ushbu kamchiliklar kritik muhim hisoblanmaydi.

Veb-interfeysga masofaviy ma’murlashni ulashdagi yengish zarur bo‘lgan to‘siq–autentifikatsiya jarayoni.

Agar ushbu mexanizm ishonchli bo‘lmasa xaker osongina uni chetlab o‘tishi va ilova yoki kompyuter ustidan nazoratga ega bo‘lishi mumkin.

Ma’lumotlarni shifrlash autentifikatsiyaning eng ommaviy

usullari-vazaviy autentifikatsiya va NTML (NT LAN Maneger). Ularni ham buzib kirish mumkin. Lokal yoki simsiz tamoqda tinglash bilan shug‘ullanuvchi xaker bazaviy identifikatsiya ma’lumotlarini ushlab qolishi mumkin va foydalanuvchi nomidan tashqari uning parolini ham osongina aniqlashi mumkin.

NTML-Micrasoftning xususiy autentifikatsiya sxemasi–veb-autentifikatsiya uchun ham ishlatilishi mumkin. NTML birmuncha xavfsizroq bo‘lsada, u “qo‘pol kuch” (grubaya sila) ishlatib xujumlanishi mumkin.

Masofadan ma’murlanuvchi tizimga kirish xavfsizligini ta’minlash uchun eng yaxshi yechim–mijoz sertifikatini tekshiruvchi SSL (Secure Sockets Layer) dan yoki ma’lumotlarni shifrlash bilan bazaviy autentifikatsiyadan foydalanish.

Xulosa

Masofadan ma’murlashning maksimal xavfsizligini ta’minlash uchun foydalanuvchidan smart–karta talab etuvchi EAP (Extensible Autensible Authentification Protocol) bazasiga virtual xususiy tarmoq infrastrukturasidan foydalaniladi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Amadi E.C., Onebunne F. C. Analysis Of Web Server Security Challenges. Iheukwumere O. Federal University Of Technology, Owerri. emmanuel.amadi@futo.edu.ng. International Journal For Research In Advanced Computer Science And Engineering. June 2016

2. Garcia-Valls, M.; Calva-Urrego, C.; García-Fornes, A. Accelerating smart eHealth services execution at the fog computing infrastructure. Future Gener. Comput. Syst. 2020, 108, 882–893. [CrossRef]

3. Monostori, L. Cyber-physical production systems: Roots, expectations and R&D challenges. Procedia CIRP 2014, 17, 9–13.

4. Garcia-Valls, M.; Dubey, A.; Botti, V. Introducing the new paradigm of Social Dispersed Computing: Applications, Technologies and Challenges. J. Syst. Archit. 2018, 91, 83–102. [CrossRef]

5. Schagen, N.; Koning, K.; Bos, H.; Giuffrida, C. Towards automated vulnerability scanning of network servers. In Proceedings of the 11th European Workshop on Systems Security, Porto, Portugal, 23 April 2018.

6. Linxuan Song and Marisol García-Valls. Improving Security of Web Servers in Critical IoT Systems through Self-Monitoring of Vulnerabilities. Beijing University of Posts and Telecommunications, Beijing 100876, China; 2018213147@bupt.cn 2 Universitat Politècnica de València, 46022 Valencia, Spain Correspondence: mgvalls@dcom.upv.es. 2 july 2022