Matej Breznik, Arnes

Zaščitimo svoje omrežje
Protect your network

Povzetek

Problematika omrežne varnosti je prisotna že dolgo. Z množičnim približevanjem medmrežja slehernemu posamezniku pa je postala še toliko pomembnejša. Priča smo širjenju medmrežja na vsakem našem koraku in s tem tudi prenosom za nas pomembnih informacij v medmrežje. Prav tako pa se spreminjajo tudi oblike običajnega druženja, saj dandanes posamezniki množično komunicirajo s pomočjo medmrežja. Zato sta naša spletna identiteta kot tudi omrežna varnost še posebej pomembni. V primeru slabe zaščite posameznika lahko zloraba privede do kraje identitete, podatkov, denarja ali celo česa hujšega.

Ključne besede: razvoj informacijske varnosti, informacijska ozaveščenost, novodobna varnostna tveganja.

Abstract

Network security problems have been around for some time. The mass adoption of the internet has increased their importance. The internet is becoming present everywhere, and information that is important to us is increasingly online. Even the ways we socialise are changing, so that today individuals communicate en masse over the internet. All of this makes web identities and network security even more important. If an individual is poorly protected, misuse could lead to the theft of identities, data, money or even something worse. The aim of the talk is to provide delegates with an insight into the threats facing network users in recent years. We will examine changes in recent years in the access points used by attackers, and will review the mechanisms that protect us. We will also study the methods used by modern attackers to gain access to our organisations' systems, and using case studies set out the key points where protection and attention are particularly important. The session will also cover modern methods of targeted attacks and refute certain myths about protection from them.

Key words: evolution of computer security, information security awareness, modern security threats

1. Uvod

S prihodom medmrežnih tehnologij v praktično vsak del našega življenja so se spremenile tudi naše vsakdanje navade. Tako danes vedno več časa preživimo na spletu, prek njega komuniciramo z znanci, splet je postal enostaven in ni več v domeni posameznikov, poznavalcev. Na ta način lahko prek medmrežja opravimo kopico reči, za katere smo v preteklosti potrebovali fizično prisotnost. Na družbenih omrežjih se srečujemo, prodajamo, česar ne potrebujemo, kupujemo, kar si želimo, ali prek medmrežja opravljamo bančne storitve. Prenos našega zasebnega življenja na medmrežje pa ni ostal neviden kriminalcem, ki se želijo z našim prihodom na splet okoristiti. Kriminalci torej bodisi izkoriščajo naše pretirano zaupanje bodisi nam podtaknejo škodljivo programsko opremo, ki jim omogoča dostop do naših najzaupnejših podatkov. Medmrežna varnost tako ni več le stvar strokovnjakov, pač pa do določene mere zadeva prav vsakogar. Če

ne sledimo in upoštevamo informacij o varni uporabi medmrežja, se nam lahko kaj hitro zgodi, da postanemo nemočna žrtev okužbe, posledično tudi kraje identitete ali morda celo denarnega oškodovanja.

2. Stanje

V preteklosti smo skrbniki omrežij doživljali omrežne napade v obliki omrežnih pregledovanj, zoper katere se je bilo mogoče zelo enostavno zaščititi s pomočjo omrežnih požarnih zidov, ki so že z enostavnimi pravili o dovoljevanju povezav le v eno smer omejili oziroma zavrnili večino škodljivega omrežnega prometa. Poleg tega je bilo mogoče okužbo sistema zelo enostavno odkriti, saj je le-ta v primeru povezovanj na svoj kontrolni strežnik uporabljala zelo enostavne nezaščitene protokole, večinoma razne derivate IRC-protokola.

V zadnjih letih pa je tako zaznava okužb sistemov kot tudi zaščita le-teh vedno večji problem. Škodljiva programska oprema namreč v vedno več primerih uporablja zapletene šifrirane mehanizme za komunikacijo s kontrolnim strežnikom. Tudi vektor vstopa škodljive programske opreme je v zadnih letih drugačen, saj je za namestitev škodljive programske opreme lahko odgovoren kar uporabnik sam oziroma njegov skrbnik sistema, ki ni poskrbel za ustrezno omejitev pravic ali opozarjanje uporabnika.

Ene najbolj znanih okužb so t. i. drive-by-download. O njih govorimo, kadar se na posameznikov sistem, ne da bi to sam želel ali vedel, sproži prenos škodljive programske opreme (t. i. malware). Treba se je zavedati, da ne gre le za ogroženost ob brskanju po straneh slabega slovesa. Napadalci namreč izkoriščajo zlorabljene uredniške dostope popolnoma legitimnih spletnih strani, ki jih najdemo ob običajnem brskanju oziroma jih morda celo redno obiskujemo. Z zlorabo dostopa ali ranljivostjo nameščene spletne aplikacije napadalci na stran podtaknejo škodljivo kodo, ki se nato izvrši na sistemu nič hudega slutečega obiskovalca.

Žal pa se je kljub skrbi uporabnika oziroma skrbnika sistema določenemu tipu ranljivosti v programski opremi le stežka izogniti; gre za t. i. zero-day ranljivosti. V tem primeru gre za ranljivosti, ki so bile odkrite in izpostavljene javnosti oziroma zaprti skupini, še preden jih je lahko proizvajalec programske opreme odpravil oziroma zanje izdal ustrezen popravek. Tako so te ranljivosti med napadalci najbolj priljubljene, saj zoper njih še ni na voljo popravkov in imajo tako za izkoriščevalce tudi določeno tržno vrednost. Posledice okužbe uporabnikovega sistema imajo lahko različne razsežnosti. Od nedolžnega poskusa prodaje lažne protivirusne programske opreme do v zadnjih letih vse pogostejše kraje podatkov z okuženega sistema uporabnika. Izpostavljena so predvsem shranjena gesla na uporabnikovem sistemu (denimo gesla za dostop do elektronske pošte, različnih spletnih storitev ...) kot tudi shranjeni podatki na uporabnikovem okuženem sistemu, ki omogočajo dostop do elektronskega bančništva.

V zadnjih letih je v javnosti veliko govora o t. i. APT-napadih,vendar je treba pri teh napadih opozoriti, da večinoma temeljijo na starih, že odkritih ranljivostih, proti katerim pa iz takšnih ali drugačnih razlogov ni bil nameščen popravek oziroma vzpostavljena ustrezna zaščita. V nekaterih primerih bi celo lahko trdili, da je edina razlika med t. i. APT-napadom in običajnim napadom v tem, da je okužba

sistema pri običajnem napadu zgolj naključje oziroma okužen sistem ni bil posebej izbran s strani napadalca. Pri APT-napadu pa gre tudi za odločenost napadalca, da bo na tak ali drugačen način vstopil v izbrani sistem. Seveda pa je treba izločiti APT-napade, pri katerih je škodljiva programska oprema prilagojena in posebej narejena za ranljivost žrtvinega sistema.

V porastu so tudi okužbe, ki se širijo prek družbenih omrežij, saj se na teh zadržuje vedno več uporabnikov. Načini okužb so različni: od škodljivih povezav, ki vodijo na prenos škodljive programske opreme, do oglasov, ki se ravno tako zaključijo s prenosom škodljive programske opreme. Postopek okužbe v tem pogledu ne predstavlja novosti, saj se ta sproži bodisi samodejno z izkoriščanjem znane ranljivosti sistema bodisi pa prepriča uporabnika, da prenese in namesti škodljivo kodo. Na ta način bi lahko prišli do zaključka, da se prevaranti in goljufi premikajo skupaj z večino uporabnikov ter obstoječe metode okužbe in prevare prilagajajo novim okoljem.

3. Ukrepi

Pred bodočimi omrežnimi tveganji se le stežka zaščitimo. Pri omrežni varnosti, kjer se grožnje in tveganja nenehno spreminjajo, je osrednjega pomena dobra informiranost omrežnega skrbnika, ki lahko s poznavanjem tendenc ustrezno zaščiti svoje omrežje in uporabnike pred okužbami, krajo gesel, osebnih podatkov in v končni fazi materialnega ali moralnega oškodovanja organizacije ali posameznika. Pri tem ne gre pozabiti tudi na osveščenost posameznikov, ki so zaposleni v organizaciji, saj lahko s svojimi dejanji v veliki meri prispevajo k varnosti organizacije ali pa jo po drugi strani ogrožajo. Zato je pomembno, da so posamezniki izobraženi vsaj do določene stopnje, na kateri so še sposobni prepoznati poskus socialnega inženiringa ter preprečiti, da bi sami postali žrtev prevare.

4. Viri

1. Bu, Z., Bueno, P., Kashyap, R., Wosotowsky, A.: The New Era of Botnets http://www.mcafee.com/in/resources/white-papers/wp-new-era-of-botnets.pdf.
2. Ducklin, P. (23. 12. 2010): Internet Explorer zero-day exploit – explanation and mitigation http://nakedsecurity.sophos.com/2010/12/23/internet-explorer-zero-day-exploit-explanation-and-mitigation/.
3. Naraine, R. (15. 4. 2009): Drive-by Downloads, The Web Under Siege http://www.securelist.com/en/analysis/204792056/Drive_by_Downloads_The_Web_Under_Siege.
4. Spletna stran: http://blog.7elements.co.uk/2011/06/apt-in-nutshell.html.