

Konferenca Bloomberg Adrie o kibernetiski varnosti

BLOOMBERG ADRIA TV, 18. 11. 2024, **ZAČETEK**, 08:23

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Digitalne grožnje so vse bolj zapletene in sofisticirane, kibernetiska varnost pa postaja ključen element uspešnega poslovanja in zaščite nacionalne varnosti na letošnjem Bloomberg Adria Cyber security Summitu bomo ta četrtek govorili o inovativnih pristopih na tem področju, strategijah za zmanjšanje tveganj ter sodelovanju med javnim in zasebnim sektorjem, sektorjem. Poudarek bo na tem, kako se podjetja in organizacije lahko pripravijo na nenehno spreminjajoče se grožnje v digitalnem okolju. O tem bodo na konferenci med drugim govoril nekdanji specialni agent FBI-ja, pa državni sekretar na obrambnem ministrstvu, predsednik uprave **NLB** in Telekoma Slovenije, tudi generalni sekretar Gen energije in še številni drugi strokovnjaki. O boju proti kibernetickemu kriminalu pa bo za Bloomberg Adrio govoril prav tako tudi gost četrtkove konference Mitja Trampuž, direktor družbe **CREAPLUS** in podpredsednik Sekcije za kibernetisko varnost pri **Gospodarski zbornici Slovenije**. Pozdravljeni gospod Trampuž.

MITJA TRAMPUŽ (sekcija za kibernetisko varnost **GZS**, podpredsednik

Lep pozdrav.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Torej kibernetiski kriminalci se vse bolj poslužujejo tudi umetne inteligence. Kakšna je na drugi strani vloga umetne inteligence in strojnega učenja pri zaščiti poslovnih sistemov?

MITJA TRAMPUŽ (sekcija za kibernetisko varnost **GZS**, podpredsednik

Drži, kriminalci se poslužujejo umetne inteligence in imajo to prednost tudi, da imajo praktično neomejena finančna sredstva, ne. Za razliko od tistih, ki branimo poslovne sisteme. No, k sreči tudi mi, ki branimo poslovne sistem, uporabljamo umetno inteligenco, gre pa zato, da umetna inteligenca je sposobna obdelovati velike količine podatkov v realnem času, potem zna prepoznati določene vzorce in pa odkriti neke nenavadne aktivnosti in s tem potem tudi lahko hitreje zaznamo določene kibernetiske grožnje. Dejstvo je, da brez umetne inteligence bi bilo nemogoče praktično danes se spopasti s kibernetiskim kriminalom in praktično že vsaka sodobna rešitev za zagotavljanje kibernetiske varnosti že na tak ali drugačen način že uporablja umetno inteligenco oziroma je vgrajena v neke vrste umetne inteligence, ki nam pomaga seveda hitreje zaznavati določene nepravilnosti, določene grožnje in potem tudi izvajati hitrejši odziv. S tem pa preprečimo tudi morebitno škodo.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Kako se pri kibernetiskih napadih uporablja na primer deep fake, pa recimo avtomatizirani phishing? Koliko je recimo napadov ko dejansko uporabnik težko ali zelo težko prepozna, na primer deep fake kot nekdo se izdaja za njegovega nadrejenega recimo na primer kako se boriti proti temu?

MITJA TRAMPUŽ (sekcija za kibernetisko varnost **GZS**, podpredsednik

Torej deep fake gre za tehnologijo, kjer zlonamerneži z neko poskušajo ustvariti pač videz prave osebe, torej poskušajo impersonirati določeno osebo in s tem izkoristi to zaupanje. Zdaj deep fake-i recimo so neka tehnika napadov, ampak v tej neki poplavi phishing napadov predstavlja relativno majhen odstotek. Torej to ni zdaj poplava teh deepfakov, je pa tako da so ti deepfaki običajno imajo, imajo neke večje finančne posledice. Jaz bi rekel, da je to mogoče samo nekaj odstotkov teh celotnih napadov. Zdaj kako se pa človek bori proti tem napadom je običajno tako da v podjetju je potrebno imeti neko urejeno poslovno okolje, se držati nekih pravil in če to upoštevamo potem je možnost uspešnega torej deep fake napada relativno majhna. Druga stvar je pa recimo tudi ničelno zaupanje. Tako imenovan Zero trust pomeni, da vedno preverimo vsakega preverimo tam kjer je to smiselno. Skratka nikomur ne zaupamo pri teh zadevah. To si pa neka taka rešitev pa v zadnjem času se seveda tudi pojavljajo rešitve za

detektiranje deep fakov, to so pa tehnične rešitve, ki to omogočajo in seveda neka taka kombinacija bi lahko praktično zmanjšala to možnost uspešnih deepfake napadov na praktično nič.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

So podjetja sicer po vašem mnenju usposobljena za boj proti recimo kibernetičnemu kriminalu, tu mislim predvsem na mala in pa srednje veliko podjetja.

MITJA TRAMPUŽ (sekcija za kibernetično varnost **GZS**, podpredsednik)

Moje mnenje je, da niso ustrezno pripravljena, zato smo tudi recimo v tem poslu še posebej majhna in srednja podjetja pri njih je očitno, da nimajo veliko kadra, ki bi se s tem ukvarjalo. Potem je tudi tukaj pomanjkanje strokovnega znanja, pa mogoče tudi pomanjkanje finančnih sredstev za to področje. In vse skupaj potem pripelje do tega, da so majhna in srednja podjetja podhranjena, kar se tiče ustrezne zaščite kibernetične varnosti. Zdaj recimo imamo večja podjetja, so finančne ustanove, potem telekomunicijski operaterji. To so recimo boljše pri njih je stanje boljše, ker seveda so tudi panožno regulirana. Je pa mogoče ta moment za omeniti, da ta večja podjetja imajo za svoje dobavitelje tudi manjša podjetja, manjša in srednja podjetja in preko teh podjetij ki niso tako dobro zavarovana potem pridejo napadi tudi v teh večjih podjetjih tako da tukaj mogoče za omeniti direktivo niz 2, ki pa začenja obravnavati tudi ta majhna in srednja podjetja, torej pardon kompletno dobavno verigo in tukaj se zajame tudi potem ta manjša in srednja podjetja, da morajo seveda dvigniti to raven svoje zaščite.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Kaj pa javna in državna uprava? Na primer tudi šolski sistem videli smo zdaj napad na Univerzo v Mariboru pred kratkim. Ali ta vlagajo dovolj v zaščito recimo tu mislim tako finančno zaščito kot tudi izobraževanje lahko vsem omenjenim koristi, morda povezovanje, na primer skupna zaščita?

MITJA TRAMPUŽ (sekcija za kibernetično varnost **GZS**, podpredsednik)

Ja omenili ste šolstvo dejansko je šolstvo bom rekel precej na udaru in kar se tiče vlaganj mislim, da je tukaj še prostora za izboljšanje. Zagotovo bi bilo treba tukaj osveščati zaposlene. In vlagati v dvig te kulture in pa seveda tudi tehnična sredstva. Mislim da recimo posebej zdravstvo, šolstvo, socialne ustanove to so področja v javni upravi, ki se mi zdi da so zelo podhranjena mogoče ministrstva, policija, vojska mislim da je tukaj stanje boljše. Kar je mogoče logično. Vidim pa da je potrebno absolutno pri vseh teh subjektih začeti na vseh področjih to pomeni od osveščanja do potem tudi nekih procesno akcijskih ukrepov in potem do neke tehnične zaščite. Konkretno recimo primer danes učitelj na osnovni šoli ima službeni prenosnik, ki pač nima nobene zaščite še niti najbolj osnovne antivirusne zaščite, proti virusne zaščite ne uporablja. Kaj šele, da bi recimo bil v nekem omrežju nadzorovanem omrežju, kjer bi imel neko odzivanje in spremljanje in pa odzivanje na kibernetične prošnje.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Se omenjeni poslužujejo varnostnih pregledov, ki jih opravljate v Kreaplusu? Kaj ugotavljate med temi pregledi?

MITJA TRAMPUŽ (sekcija za kibernetično varnost **GZS**, podpredsednik)

Torej varnostni pregledi so namenjen temu, da najdemo pomanjkljivosti. V določenih informacijskih sistemih je to 1 od ključnih ukrepov, zato, da se seveda lahko izboljšamo, torej z varnostnim pregledom ugotovimo, kje so naše pomanjkljivosti. Zdaj običajno mogoče ena taka svetla točka so bili vavčerji v Sloveniji, s katerimi so bila podjetja motivirana, da izvedejo določene varnostne preglede, ne, in ugotovijo, kje so njihove šibke točke. Takoj zatem, ko so ti vavčerji potem bili zaključeni, se seveda je, to je praktično ponehalo, so ti varnostni pregledi niso več tako aktualni, zdaj se izvajajo samo pri tistih večjih podjetjih, ali pa omogoče tistih, ki obdelovalci nekih osebnih podatkov ali pa recimo ponudniki digitalnih storitev tam, kjer se to potrebno. Tam so, to izvaja, medtem ko v manjših in srednje velikih podjetjih pa mislim, da ni tega. Je pa mogoče za omeniti, da obstaja ta trenutek. Zdaj že obstaja že rešitve za avtomatizirano izvajanje varnostnih pregledov in vdornih testov, kar je tudi potem cenovno bolj sprejemljivo. Izvaja se jih periodično, ne samo 1 na leto, kot je do zdaj bila praksa, ampak se jih lahko izvaja tudi vsak mesec, vsak teden, poleg tega pa mogoče običajno tudi simulacije nekih kibernetičnih napadov, kot da bi torej bili napadeni in s tem mi vidimo, kje so recimo luknje v naših informacijskih sistemih in jih lahko seveda kar dobimo iz teh rešitev, tudi potem nekaj navodila, kako to odpraviti, te pomanjkljivosti in skratka dobimo neke vrste pomoč, da lahko zagotovimo neke vrste kibernetično odpornost.

Trajanje: 10:00

3 / 3

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Čisto na kratko v dveh stavkih zaostajamo po zaščiti za razvitejšimi državami?

MITJA TRAMPUŽ (sekcija za kibernetško varnost **GZS**, podpredsednik)

Kar se tiče, bom rekel, da izpostavljeni smo čisto enakim grožnjam kot so ostali razvitih zahodnih državah. Kar bi mogoče izpostavil, je, da se mogoče premalo zavedamo ali pa je premajhna osveščenost uporabnikov. Je pa mogoče en tak zanimiv element in to je, da so recimo zavarovanja kibernetških tveganj so praktično, ne obstajajo v Sloveniji oziroma so na zelo nizkem nivoju. Pa kar je mogoče za opaziti je, da se v Sloveniji v primerjavi z drugimi državami, zahodnimi državami se mogoče ta tveganje kibernetške varnosti ne obravnavajo kot poslovna tveganja. In to je v zahodnih državah že v bistvu postalo, kot bom rekel top 3. Med top tremi tveganji v Sloveniji pa recimo tveganje kibernetške varnosti zaenkrat še ni obravnavana tako kot bi si recimo zaslužila.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

Velja hvala za pogovor gospod Trampuž, seveda več pa tudi v četrtek na konferenci.

MITJA TRAMPUŽ (sekcija za kibernetško varnost **GZS**, podpredsednik)

Hvala tudi vam.

MARTIN TOMAŽIN (voditelj, Bloomberg Adria)

O boju proti kibernetškemu kriminalu je za Bloomberg govoril Mitja Trampuž, direktor družbe Kreaplus in podpredsednik sekcije za kibernetško varnost pri **GZS**.