

Intervju

Jacopo Zorzin Mladi izvedenec s področja kibernetske varnosti dobro pozna grožnje ter ukrepe in prakse za zaščito računalniških sistemov, omrežij in podatkov pred nepooblaščenim dostopom, krajo ali zlorabo

»Najbolj podcenjena grožnja je človek«

Svetlana Breclj
Veronica Piredda

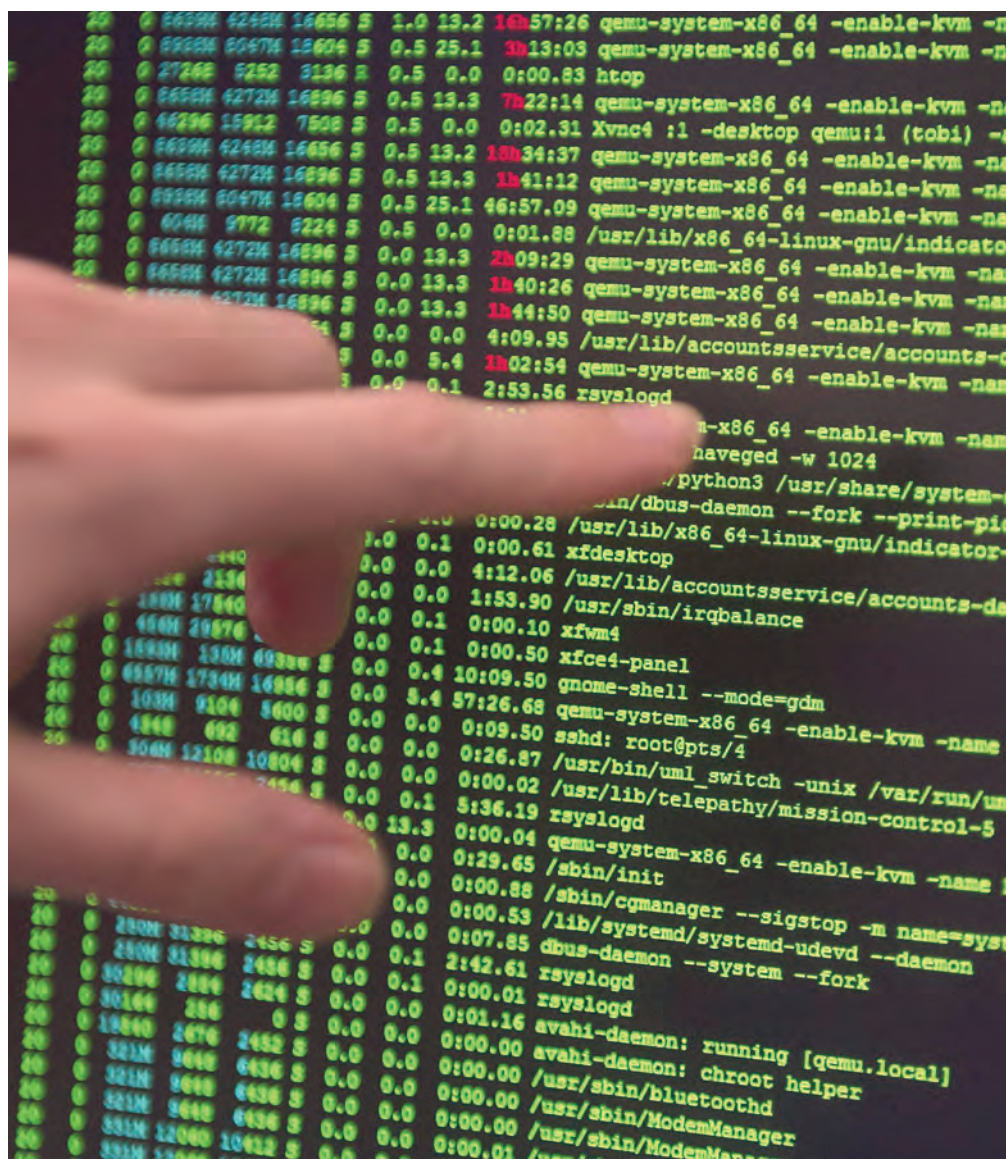
MILAN Kibernetska varnost (angl. *cybersecurity*) zajema tehnologije, ukrepe in prakse za zaščito računalniških sistemov, omrežij in podatkov pred nepooblaščenim dostopom, krajo ali zlorabo. Vključuje tehnične rešitve, kot so protivirusni programi in sistemi za odkrivanje vdorov, ter organizacijske ukrepe, kot so varnostne politike, izobraževanje zaposlenih in redno spremljanje groženj. Napadi lahko povzročijo hude posledice: krajo osebnih ali finančnih podatkov, motnje v delovanju podjetij, izgubo zaupanja strank, finančno škodo in pravne težave.

Približno 80–95 odstotkov kibernetskih napadov se začne s t. i. *phishingom* oziroma ribarjenjem ali drugimi lažnimi sporočili, kar poudarja ranljivost uporabnikov. Zaradi tega je ključnega pomena celostna zaščita, ki združuje tehnologijo in človeški dejavnik. Evropska unija je temu področju namenila jasen pravni okvir. GDPR oziroma *Splošna uredba o varstvu podatkov* določa, kako se smejo zbirati, obdelovati in varovati osebni podatki, ter nalaga obehnost poročanja o incidentih. Direktiva NIS2 pa postavlja minimalne standarde varnosti za kritično infrastrukturo in krepi sodelovanje med državami članicami, s čimer organizacije postanejo bolj odporne proti grožnjam in zmanjšajo tveganje škodljivih napadov.

Da bi bolje spoznali aktualno temo kibernetske varnosti in razumeli, kako se podjetja danes spopadajo z digitalnimi grožnjami, smo nekaj vprašanj postavili Jacopu Zorzinu. Jacopo, star 24 let, dela za milansko podjetje Deda Group, natančneje v oddelku Deda Tech. Študiral je na Pomorski akademiji Jadrana (Accademia Nautica dell'Adriatico) v Trstu, opravil ITS oziroma program iz kibernetske varnosti, trenutno pa nadaljuje dodiplomski študij varnosti informacijskih sistemov in omrežij na Univerzi v Milanu.

Jacopo, kako uporaba umetne inteligence danes spreminja napade ribarjenja?

Ribarjenje oziroma *phishing* je razmeroma preprosto, a zelo razširjen kibernetski napad. Napadalec pošlje elektronsko sporočilo, ki je zasnovano tako, da deluje čim bolj verodostojno in uporabnika prepriča o kliku na povezavo. Ta vodi na lažno spletno stran, na kateri neizkušen uporabnik vnese svoje osebne ali dostopne podatke. Napad pogosto uspe prav zaradi zaupanja uporabnikov in nezadostnega prepoznavanja sumljivih spletnih naslovov, zato sta ozaveščenost in izobraževanje ključni deli obrambe.



Kibernetska varnost Ključnega pomena je celostna zaščita, ki združuje tehnologijo in človeški dejavnik ANSA

pne podatke. Napad pogosto uspe prav zaradi zaupanja uporabnikov in nezadostnega prepoznavanja sumljivih spletnih naslovov, zato sta ozaveščenost in izobraževanje ključni deli obrambe.

Umetna inteligenca pri ribarjenju ne spreminja koncepta napada, temveč ga naredi hitrejšega in učinkovitejšega. Omogoča ustvarjanje bolj prepričljivih vsebin in s tem povečuje verjetnost, da uporabnik nasede digitalni prevari.

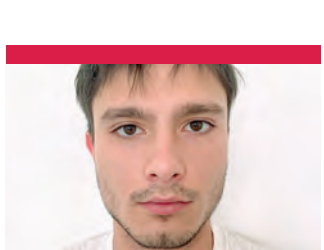
Katera kibernetska grožnja je danes po mnenju podjetij najbolj podcenjena?

Najbolj podcenjena kibernetska grožnja v podjetjih je človek. Kljub tehnološki zaščiti so neizobraženi zaposleni najlažja tarča napadalcev. *Phishing* ostaja najpogostejši napad in glavni vstopni vektor, kar se v praksi potrjuje vsak dan.

Kako pripravljeni so današnji sistemi kibernetske varnosti na obvladovanje različnih napadov?

Pristop podjetij h kibernetski varnosti je močno odvisen od njihove velikosti, vrste in dr-

žave. V Italiji se problem pogosto podcenjuje, medtem ko v ZDA, na Irskem ali Kitajskem varnost dojemajo veliko resneje. Mala in srednja podjetja so pogosto nepripravljena: nimajo vzpostavljenih varnostnih sistemov, zaposleni niso izobraženi, in če ni navdušenega IT-tehnika, se



» Umetna inteligenca povečuje verjetnost, da uporabnik nasede digitalni prevari

Jacopo Zorzin
Izvedenec za kibernetsko varnost

običajno ne uvede nič več kot osnovni protivirusni program, ki pa ni dovolj. Zaradi pomanjkanja sredstev, časa in kadrov se varnost pogosto upravlja le reaktivno, šele po nesreči, ko podjetja spoznajo, kako ključna je.

Kako pomemben je danes človeški dejavnik v primerjavi s tehnologijo pri zagotavljanju varnosti?

Človek je temelj varnosti – sistem je močan toliko, kolikor je močan njegov najšibkejši člen. Kljub naprednim sistemom lahko nepazljiv uporabnik ali zastarela programska oprema hitro povzroči vdor. Približno 90 odstotkov napadov se začne prek e-pošte ali okuženih naprav, saj nadzori pogosto niso dovolj močni. Če bi uporabniki poznali osnovna pravila prepoznavanja sumljivih sporočil in spletnih strani, bi bili bistveno varnejši.

Zavedanje in izobraževanje zaposlenih sta torej ključna za zmanjšanje tveganja kibernetskih napadov, saj kombinacija tehnologije in ozaveščenih uporabnikov zagotavlja učinkovito zaščito.

Instagram

@direkt_pd #bodidirekten

Meme Damir Terčon
Komentarji Francesco Petaccia



Bodimo zmeraj direktni!



Sodelavke in sodelavci mladinske strani @Direkt: Svetlana Breclj, Julija Cante, Martina Cavotta, Nika Maria Costantin, Marco D'Errico, Malina Dolhar, Lapo Farolfi, Emil Favento, Mila Gergolet, Tadeja Gergolet, Sara Hlabian, Elisabetta Lovero, Martin Kits Nieuwenkamp, Francesco Petaccia, Veronica Piredda in Damir Terčon. Pridruži se nam! Z nami stopi v stik prek Instagrama. Beri nas vsak petek.

V prestolnici Festival slovenskih univerz

LJUBLJANA Na Gospodarskem razstavišču v Ljubljani bo danes in jutri od 9. do 18. ure potekal Festival slovenskih univerz. UNI-SI je sejemsko zasnovan dogodek, ki dijakom in dijakinjam ponuja predstavitev vseh fakultet osmih slovenskih univerz. Obiskovalci bodo lahko pridobili informacije o vpisnih postopkih in se o svoji študijski poti pogovorili s študenti, ki bodo z njimi delili izkušnje iz prve roke. Študijski programi bodo razdeljeni po posameznih področjih, kar bo še dodatno olajšalo izbiro.

Vstop je prost! Več informacij najdete na spletni povezavi festival-uni.si.
Sara Hlabian