INTERVJU: Nađa Halebić, tehnična direktorica sarajevskega družinskega podjetja ALEM Sistem

V Sloveniji se že počutimo kot doma

Pandemija je sarajevsko IT-podjetje ALEM Sistem spodbudila, da svoje znanje ponudi tudi zunaj meja Bosne in Hercegovine. Že doslej so se lahko pohvalili z veliko projekti v različnih državah, tudi v Nemčiji, lani pa so se odločili, da bodo v p(Evropski uniji#Evropska unija) uradno odprli še svojo pisarno. Izbrali so Ljubljano, k čemur je med drugim pripomoglo dejstvo, da na področju varnostnih rešitev p(IBM#IBM) že dolgo sodelujejo s podjetjem p(Alterna#Alterna) distribucija. O tem, kako jih je sprejel slovenski trg, o izzivih kibernetske varnosti in načrtih smo se pogovarjali s tehnično direktorico Nađo Halebić, ki podjetje vodi skupaj s svojim bratom.

Zakaj ste se odločili za ustanovitev pisarne v Sloveniji?

Skozi vrsto projektov, ki smo jih izvajali v regiji, smo prepoznali potrebo po znanju in idejah, ki jih imamo. Pandemija nas je skoraj silovito potisnila v spletni slog življenja in s tem odprla vrata kibernetskim izzivom, ki so bili prej precej pod radarjem. Potreba po storitvah kibernetske varnosti se je povečala in tako smo ocenili, da je pravi čas, da svoje znanje in storitve ponudimo zunaj Bosne in Hercegovine. Zato smo odprli pisarno v Ljubljani.

In kakšne so vaše prve izkušnje pri nas?

Iskreno povedano, se že počutimo kot doma. Pri nas imamo rek, da se dober glas sliši daleč stran, pri vas pa dober glas seže v deveto vas. In prav to se nam dogaja. Čeprav se s potencialnimi strankami pogovarjamo prvič, nam pogosto povedo, da so že slišali za nas. Verjetno je to posledica sodelovanja z našima dolgoletnima partnerjema Alterna Distribucija in IBM, s katerima tesno sodelujemo v regiji in na trgu BiH.

Kaj za vas na področju uvedbe varnostnih rešitev IBM pomeni partnerstvo s podjetjem Alterna distribucija?

> **Pandemija je samo pospešila proces univerzalne digitalizacije poslovnih procesov, ki se je neizogibno bližal. Tehnološko smo pripravljeni, da sprejmemo to preobrazbo, sistemsko in varnostno pa sploh ne.**

Menimo, da je pomembno, da se obkrožimo z ljudmi, ki imajo enake vizije in cilje kot mi. Prav to smo našli pri podjetjih Alterna distribucija in IBM. Naši uspešno končani projekti so najboljši kazalnik tega.

Kaj vaš prihod na slovenski trg pomeni za širitev na ostale trge EU?

Odprtje pisarne v Ljubljani je prvi korak k uresničitvi naših načrtov za vstop na trge drugih držav EU. Čeprav nam ti trgi niso tuji in smo pri nekaterih navzoči že leta, menimo, da je pravi čas, da se uradno predstavimo s projekti, ki bodo pod okriljem naše pisarne v Ljubljani.

Katere storitve pa ponujate v Sloveniji?

Trenutno se osredotočamo na storitve kibernetske varnosti, ki vključujejo storitve testiranja PEN, iskanje, kategorizacijo in pregled ranljivosti v IT-okolju ter usposabljanje in izobraževanje uporabnikov za posebne varnostne izzive. Ponujamo tudi storitve najema našega notranjega varnostnooperativnega centra ter storitve prodaje, uvedbe in konfiguracije varnostnih rešitev IBM.

Katere so vaše glavne konkurenčne prednosti? Menda zelo veliko vlagate v usposabljanje zaposlenih oziroma v zaposlene nasploh.

Tako je. Čeprav se naše geslo glasi »Dokler bo trajalo naše potovanje, je pomembno, da se imamo lepo«, svojega dela ne jemljemo kot samoumevnega. Verjamemo, da do uspeha vodita le iskren trud in ljubezen do tega, kar počnemo. Zato vsakega člana naše ekipe spodbujamo k nenehnemu učenju in pridobivanju novih znanj. Odlikujeta nas timsko delo in predanost, na kar smo zelo ponosni. Zelo pomembno je tudi praktično znanje, ki ga pridobimo z zanimivimi projekti. V posebnih razmerah, ki nastajajo v okviru projektov kibernetske varnosti, pogosto pride do izraza iznajdljivost. Ko poskušamo prelisičiti hekerja, imamo praktične in zanimive ideje, ki celoten proces naredijo več kot zanimiv - podobno kot pri šahovski igri.

Kakšno pa je stanje na področju IT-kadrov v BiH? V Sloveniji njihovo pomanjkanje označujejo kot eno največjih težav IT-panoge.

Razmere so zelo podobne. Najti zadostno število IT-kadra je velik izziv, še posebej zato, ker se mladi IT-inženirji najpogosteje odločajo za delovna mesta v programiranju in pri sistemskih integratorjih. Za kibernetsko varnost čas šele prihaja.

Katera področja kibernetske varnosti so trenutno najbolj aktualna, kje imajo podjetja največ težav?

Zaščita podatkov pred nepooblaščenim dostopom in protipravnim prisvajanjem je pogosta težava vseh podjetij v regiji in državah EU. V EU so zahteve po skladnosti z GDPR visoko na seznamu prednostnih nalog in so zato nepogrešljiv člen v varnostni politiki vsakega poslovnega procesa. Vendar je skladnost le eno izmed perečih varnostnih vprašanj. Z uvedbo spletnega poslovanja oziroma dela od doma postaja zaščita pred hekerskimi napadi vedno bolj zanimiva in nujna. Mislim, da bomo letos na slovenskem trgu imeli veliko rast hekerskih napadov, saj se je igrišče za hekerje zelo razširilo.

Kako je pandemija spremenila področje kibernetske varnosti?

Pandemija je samo pospešila proces univerzalne digitalizacije poslovnih procesov, ki se je neizogibno bližal. Tehnološko smo pripravljeni, da sprejmemo to preobrazbo, sistemsko in varnostno pa sploh ne. Ko danes analiziramo odziv podjetij na pandemijo, lahko opazimo, da gre za proces, ki je potekal v več fazah. Prva faza je prisilila podjetja, da so hitro razmišljala o tem, kako prilagoditi svoje poslovanje novim razmeram. Za to fazo so bili značilni nakupi prenosnikov in tabličnih računalnikov ter prehod na oblačne rešitve za pisarniška orodja. Druga faza se je nato osredotočila na trajnost poslovnih procesov in njihovo kontinuiteto. Podjetja so v tej fazi razmišljala, kako zagotoviti oddaljen dostop do virov. Iskali in kupovali so rešitve za povezave VPN. To je odprlo vrata v tretjo fazo, v kateri smo trenutno. Gre za zaščito podatkov in virov. Kibernetska varnost je v strokovnih krogih postala vsakodnevna tema, vsak dan poslušamo o novih hekerskih napadih, zlorabi oddaljenega dostopa do virov in kraji osebnih in občutljivih podatkov. Najbolj zaskrbljujoče je, da proti temu ni nihče imun, ne majhna podjetja z nekaj zaposlenimi ne tista z več tisoč zaposlenimi.

Kako ste se novim razmeram prilagodili v svojem podjetju?

Mislim, da lahko kar s ponosom povem, da smo svoje sile zelo hitro konsolidirali in preprosto napredovali v skladu z novimi razmerami. Če sem povsem iskrena, je bil večji izziv, kako naše zaposlene zaščititi pri neposrednih stikih s strankami, saj morajo zaradi narave dela velik del svojih nalog opravljati na lokaciji stranke.

Katere so glavne prednosti varnostnih rešitev IBM?

Zavzetost in nenehen razvoj sta dve značilnosti varnostnih rešitev IBM. Kibernetska varnost je zahtevna veja informacijske tehnologije, pri kateri se spremembe edina stalnica. Hitre spremembe, vrste in načini hekerskih napadov, vrste orodij in metod, ki jih uporabljajo, so zadosten izziv za kategorizacijo resnosti vsakega proizvajalca varnostnih rešitev. Izboljšanje varnostnih odzivov na trenutne varnostne izzive je že samo po sebi dovolj zapleteno. Resnost IBM kot vodilnega proizvajalca varnostnih rešitev se kaže v številnih dodatnih storitvah, ki jih ponuja svojim strankam za boljšo zaščito in servis. Tu je zlasti treba omeniti laboratorij IBM X Force, katerega naloga je, da nenehno preiskuje nove potencialne grožnje in ranljivosti v vodilnih informacijskih sistemih ter zanje ustvari ustrezne varnostne odzive in zaščito. Ta storitev je del skoraj vseh varnostnih rešitev IBM in je nepogrešljiv člen v boju proti kibernetskemu kriminalu.

Na splošno velja prepričanje, da so rešitve IBM primerne predvsem za velika podjetja. Kako je s tem pri varnostnih rešitvah, kakšna je ponudba IBM za manjša podjetja?

Portfelj varnostnih rešitev IBM je precej širok in tudi zelo prilagodljiv. Po drugi strani pa je specifikacija in izvedba vsake varnostne rešitve odvisna od znanja in vizije izvajalca. Zelo pogosto smo prilagajali in spreminjali standardne konfiguracije, da smo ugodili posebnim zahtevam in potrebam naših uporabnikov. Zaradi prilagodljivosti orodij smo bili pri tem vedno uspešni. Številne naše stranke spadajo v skupino srednjih podjetij in na to smo še posebej ponosni.

Kdo je Nađa Halebić

Nađa Halebić je skupaj s svojim bratom druga generacija, ki vodi družinsko podjetje ALEM Sistem. V podjetju, ki je bilo del njenega odraščanja, je že več kot 20 let, pot do mesta tehnične direktorice pa je trajala 15 let. V tem času je svoje znanje gradila od najosnovnejših nalog postavitve in oblikovanja omrežnih okolij do upravljanja rešitev za zaščito pred izgubo podatkov za velike mednarodne banke, kakršna je Deutsche Bank. Poleg poklicne je zgradila tudi akademsko kariero. Končala je magistrski študij na oddelku za računalništvo in informatiko na fakulteti za elektrotehniko v Sarajevu. Del akademske kariere je na tej fakulteti preživela tudi kot asistentka pri predmetih oblikovanje informacijskih sistemov in raziskave operacij. Kot pravi, je tudi zelo ponosna mama dveh otrok, v prostem času pa uživa v jogi in meditaciji.

O podjetju ALEM Sistem

Družinsko podjetje ALEM Sistem so v Sarajevu ustanovili junija 1996. Cilj je bil na trg BiH prinesti nove ideje iz segmenta IT-tehnologij. Blagovno znamko so zgradili na profesionalnih in etičnih normah, pri čemer so dali poseben poudarek timskemu delu in skupnosti. »Naša uspešna varnostna zgodba se je začela spontano, vendar je kmalu postala glavni fokus našega delovanja na trgu IT,« je povedala tehnična direktorica Nađa Halebić. Danes je ALEM Sistem po njenih besedah zasnovan kot »security boutique shop«, ki ponuja svetovanje na področju kibernetske varnosti, ki temelji na storitvah modre, rdeče in vijolčaste ekipe. V svojih vrstah imajo certificirane etične hekerje, svetovalce za kibernetsko varnost in integratorje rešitev za kibernetsko varnost.

»Naše zavezo, da bomo postali vodilno podjetje za kibernetsko varnost v jadranski regiji, so prepoznali tudi naši partnerji, zlasti Alterna Distribucija in IBM, ter se nam pridružili na poti skozi izzive kibernetske varnosti,« je povedala Halebićeva. ALEM Sistem je bilo eno prvih podjetij v regiji, ki je pridobilo certifikat za rešitev IBM SOAR Resilient, certificirani pa so tudi za rešitve IBM Guardium, IBM QRadar SIEM in rešitve, povezane z omrežnimi okolji.

Na njihovem seznamu referenc so številni zanimivi projekti v različnih priznanih podjetjih. Varnostne rešitve so med drugim uvajali v nemški Deutsche Bank, bolgarski Bulbank Sofia, v SBB Srbija, Telemachu Slovenija, BH Telecomu Sarajevo, Sberbanki Sarajevo, NLB banki Sarajevo, Unicredit Banki Mostar in v več drugih podjetjih.