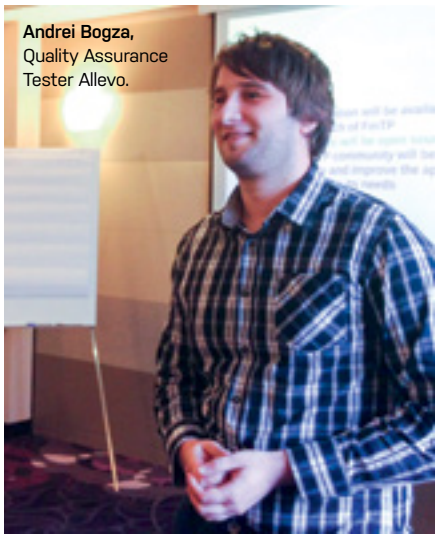
De ce au nevoie companiile de **specialiști în securitate informatică?**

Explozia din ultimii ani a dispozitivelor mobile și a serviciilor oferite prin Internet ne-au transformat într-un mod spectaculos activitățile din viața de zi cu zi. Comunicăm la orice oră, avem acces instant la orice informație sau facem cumpărături fără a păși fizic într-un magazin. Într-o companie, angajații din locații diferite pot comunica, colabora și partaja documente ca și cum ar fi în același birou iar cloud-ul devine una din cele mai populare modalități de stocare a informației, reducând infrastructura necesară desfășurării activității unei companii. Acest boom tehnologic a avut și un efect negativ prin creșterea atacurilor și infracțiunilor informatice, ale căror victime sunt persoane, companii sau chiar state. Securitatea informatică a devenit un domeniu de un dinamism extraordinar. În fiecare zi sunt descoperite noi buguri, exploit-uri sau coduri malițioase iar specialiștii în domeniu trebuie să se țină la curent permanent cu tot ce e nou pentru a împiedica un potențial atac sau a limita pagubele produse.

Ideea de securitate informatică a avansat destul de rapid în ultima perioadă, până recent ea fiind centrată în jurul administratorului IT. În sarcina acestuia erau firewall-ul, antivirusul, instalarea ultimelor update-uri pentru sistemul de operare sau aplicaţiile folosite şi întreaga politică de securitate IT a companiei. Nici aceste măsuri nu sunt de trecut cu vederea însă ele oferă doar o protecţie pasivă. Astfel, a apărut şi s-a format specialistul în securitate informatică, al cărui rol este să prevadă aceste riscuri, acţionând uneori chiar din perspectiva unui atacator, să descopere punctele slabe ale sistemului informatic şi să elaboreze un plan de evitare a unei potenţiale expuneri. Tot în sarcina acestuia revine şi actualizarea continuă a politicii de securitate în concordanţă cu ultimele dispozitive sau servicii care se integrează în infrastructura companiei dar şi educarea directă a angajaţilor pentru a asigura aplicarea eficientă a acesteia.

Ceea ce observăm este că un specialist în securitate informatică, spre deosebire de administratorul IT, are un rol mult mai extins şi este necesară o flexibilitate mai mare pentru a ţine pasul cu noile ameninţări apărute zilnic. Totodata, este nevoie de un anumit nivel de dedicare şi disponibilitatea de a învăţa zilnic lucruri noi, însă efectul pe termen lung este unul cât se poate de benefic pentru compania în care acesta activează. Aici vă pot da un exemplu din compania din care fac parte (Allevo). Datorită naturii activităţii noastre (dezvoltarea de aplicaţii software destinate instituţiilor financiar bancare şi corporaţiilor), securitatea informatică a fost întotdeauna un subiect de actualitate şi de o importanţă deosebită. Asigurarea confidenţialităţii datelor dar şi garantarea siguranţei produselor software oferite au fost principalele obiective pe care ni le-am propus dar şi care ne-au convins de necesitatea unei echipe de specialişti în securitate informatică. Dovada succesului pregătirii acestora o constituie atingerea cu succes a obiectivelor propuse dar şi decizia începerii demersurilor necesare pentru obţinerea certificării de securitate ISO 27001.



Andrei Bogza,
Quality Assurance
Tester Allevo.

Revenind la nevoia de specialişti în securitate informatică, putem trage concluzia că aceştia nu mai reprezintă o componentă opţională ci una vitală iar companiile trebuie să conştientizeze riscurile la care se expun şi să investească în experti capabili să le asigure protecţia proprietăţii intelectuale şi a infrastructurii companiei, prin stabilirea unui nivel de securitate adecvat în care să-şi desfasoare activitatea aceasta.