ITCHANNEL

NR. 8, ANUL 3 • IULIE-AUGUST 2015 • www.ITChannel.ro • IT MAGAZINE FOR TOMORROW

veracomp

NOUA FAȚĂ A SECURITĂȚII IT

WhiteHat SECURITY

RSA

f5 NETWORKS

Interviu cu Sergiu Banyai,

Business Development Manager, Veracomp

>>> pag.4-5

O nouă etapă în evoluția companiei Intergraph

>>> pag.6-7

Amadeus - cum vom călători în 2030?

>>> pag.8-9

Noua strategie Symantec

>>> pag.20

techhub

The community & workspace for tech entrepreneurs

Join the TechHub Bucharest community

and get access to:

- a large international network of tech entrepreneurs & startups
- great advice from industry specialists
- local & international investors
- free, weekly events on relevant subjects
- quality networking

Bucharest.TechHub.com

ÎNTREABĂ EXPERȚII ITCHANNEL!

www.itchannel.ro/AskExperts

Robert KOMARTIN
Enterprise Application Software

Viorel ALEXANDRU
Web & Application Development

Mihai MADUSSI
Microsoft Dynamics NAV & AX

Paul ROMAN
Exchange Server and Collaboration

Ioana RENȚEA
Financial Management Systems

Dragoș MĂNAC
Cloud Computing

Mihai MUNTEANU
Networking

SUB SEMNUL SECURITĂȚII IT

Silviu COJOCARU
Redactor-șef ITChannel

În acest număr, ne-am propus împreună cu unul dintre experții din domeniu (Sergiu Banyai – Business Development Manager la Veracomp) să facem o analiză a domeniului securității IT.

Organizațiile sunt tot mai expuse la atacurile cibernetice, fiind vizate tot mai des și sistemele foarte complexe care nu puteau fi penetrate în trecut (e.g. sisteme informatice utilizate în domeniile militar sau bursier). S-a schimbat și scopul acestor atacuri cibernetice, acestea având astăzi ca scop furtul de informații și de resurse financiare. De asemenea, unele dintre atacuri se încadrează în categoria de terorism cibernetic, putând conduce la pagube imense pentru organizații sau chiar pentru state de pe glob. Diversificarea modului în care sunt realizate atacurile cibernetice, dar și avansul tehnologic, au condus la apariția unor noi categorii de soluții de securitate, după cum se poate vedea și din interviul cu Sergiu Banyai.

De asemenea, publicăm rezultatele studiului Internet Security Threat Report 2015, unul dintre cele mai complete studii de securitate publicat de o companie la nivel global. Raportul Symantec arată că cinci din şase companii mari au fost vizate de atacuri cibernetice în 2014, o creştere de 40% faţă de anul precedent. În 2014 au existat în total 24 de vulnerabilităţi de tip zero-day, lăsând câmp deschis atacatorilor pentru exploatarea breşelor cunoscute înainte de aplicarea patch-urilor.

O particularitate a fost precizia atacurilor de anul trecut, care au folosit cu 20% mai puţine emailuri pentru a-şi atinge ţintele şi au încorporat mai multe atacuri de tip drive-by download şi alte tipuri de atacuri web.

ITCHANNEL

EDITOR

ITChannel Communications
str. Burdujeni nr.7, sector 3
cod 032727
București

CONTACT
Telefon: 031 420 78 73
Mobil: 0729 777 404
E-mail: *redactie@itchannel.ro*
Web: *www.itchannel.ro*

REDACȚIA
Silviu Cojocaru (*silviu@itchannel.ro*)
Camelia Cojocaru (*camelia@itchannel.ro*)
Ștefania Dinu(*stefania@itchannel.ro*)
Bogdan Marchidanu
Marian Teodorescu (Foto Editor)

TIPĂRIT LA
Tipografia EVEREST
office@everest.ro
www.everest.ro
ISSN 2285 – 4967

NOUA FAȚĂ A SECURITĂȚII IT

Pe parcursul zilelor în care am redactat acest articol, agențiile de presă anunțau că hackerii au preluat controlul asupra rachetelor Patriot staționate în Turcia. În aceeași zi, bursa de pe Wall Street a căzut, se pare, în urma unui atac al grupului de hackeri Anonymous. Lumea IT s-a schimbat radical, societatea fiind tot mai dependentă de infrastructura informatică. Fără îndoială, acum cinci ani nu puteam discuta despre atacuri care să afecteze sisteme și organizații atât de critice. Despre modul în care s-a schimbat securitatea IT în ultimii ani, am stat de vorba cu dl. Sergiu Banyai, Business Development Manager – Veracomp Europe.

"Când vorbim despre cybersecurity, de fapt vorbim despre noile atacuri și metode apărute. Atacurile au evoluat foarte mult în ultimii ani, de la atacuri brute la atacuri sofisticate de tip APT (n.r. Advanced Persistent Threat). De asemenea, în ultimul timp putem vorbi despre atacuri orchestrate de grupări politice. În climatul geopolitic existent, România poate deveni o țintă a acestui nou tip de atac." a declarat Sergiu Banyai despre evoluția tehnologiei folosite de atacurile cibernetice.

Domeniul financiar-bancar este, de asemenea, vizat de atacuri cibernetice: *"Faptul că gradul de sofisticare a atacurilor a crescut este foarte evident în sectorul bancar. Se observă evoluția clară, de la atacurile cu troieni (e.g. Zeus, Citadel sau Conficker), la variante de atacuri personalizate pentru anumite bănci, ca și exemplu fiind multiplele atacuri din 2014 și 2015 ale malware-ului Dyre, precum și varianta actuală de J.Bot. Atacurile direcționate indică o cunoaștere foarte bună de către atacatori a măsurilor de protecție existente în infrastructura atacată. Este vizibilă o altă tendință care va evolua rapid, și în Romania dealtfel, și anume atacurile asupra sistemelor de operare și a aplicațiilor dispozitivelor mobile."* a precizat Sergiu Banyai.

Securitate la nivel de cod sursă

Diversificarea modului în care sunt realizate atacurile cibernetice, dar și avansul tehnologic, au condus la apariția unor noi categorii de soluții de securitate. Gama WhiteHat, intrată recent în portofoliul Veracomp, este dedicată testării vulnerabilităților aplicațiilor și procesului de Security Code Review. Practic, acest gen de soluții permit o testare continuă a codului sursă a programelor, începând cu faza de proiectare și încheind cu etapa de utilizare în producție a aplicațiilor.

"Soluțiile WhiteHat sunt utilizate pentru testarea aplicațiilor complexe Web (expuse pe Internet prin intermediul protocoalelor HTTP – Hyper Text Transfer Web și Secure HTTP), țintind astfel mai multe verticale profesionale. Un exemplu este cel aplicațiilor de online banking, care sunt foarte dinamice și presupun modificări multiple la intervale relativ scurte. WhiteHat oferă testarea continuă a acestor aplicații și ajută la eliminarea breșelor de securitate, pentru multiplele actualizări aplicate acestor sisteme. De asemenea, prin soluțiile WhiteHat țintim și alte categorii de clienți: site-urile de comerț electronic, casele de software și clienții acestora, precum și unele instituții guvernamentale care au procese de tip e-guvernare (sisteme online de plăți și taxe,

„Când vorbim despre cybersecurity, de fapt vorbim despre noile atacuri și metode apărute. Atacurile au evoluat foarte mult în ultimii ani, de la atacuri brute la atacuri sofisticate de tip APT (n.r. Advanced Persistent Threat). De asemenea, în ultimul timp putem vorbi despre atacuri orchestrate de grupări politice. În climatul geo-politic existent, România poate deveni o țintă a acestui nou tip de atac ”

Sergiu Banyai

depunerea declarațiilor fiscale etc.) a precizat Sergiu Banyai.

Cloud computing vs. On premises

Majoritatea firmelor IT oferă atât soluții tradiționale *on premises*, cât și soluții în *cloud*. Am discutat cu Sergiu Banyai despre oportunitatea de a investi într-una dintre cele două modalități de infrastructură, cu plusurile și minusurile aduse de acestea în organizații.

"Consider că, dacă o companie poate investi în propria infrastructură IT și deține personalul dedicat pentru administrarea acesteia, atunci fără îndoială trebuie să aleagă varianta <<on premises>>. Dincolo de calculele financiare (tradiționalul <<război>> între CAPEX și OPEX), soluțiile on premises vor oferi companiilor un control total asupra infrastructurii. Soluțiile cloud nu asigură un control asupra infrastructurii, ceea ce poate constitui un factor de risc în anumite situații. Totuși, soluțiile cloud computing pot constitui o alternativă pentru companiile care nu au resurse financiare sau umane pentru a dezvolta sau a administra propria infrastructură." a precizat Sergiu Banyai.

O altă tendință, identificată pe zona de infrastructură și securitate IT, este orientarea producătorilor IT spre dezvoltarea de echipamente de tip appliance.

"Appliance-urile sunt soluții specializate și mult mai performante pentru anumite task-uri. Spre exemplu, << load balancing>> se poate realiza, pentru un anumit volum de trafic si numar de connexiuni, folosind servere Linux (ex: NGINX sau LVS). Atunci când traficul crește semnificativ,sau in cazul unui atac la nivel de aplicatie (ex. atacurile de protocol SSL), serverul Linux va fi <<sufocat>> de aceste task-uri. În acest context, soluțiile appliance de tip ADC (Application Delivery Network) si solutiile WAF (web application firewall) de la F5 Networks preiau funcțiile de load balancing de la serverul de aplicații și adaugă optimizări avansate (caching pentru Web, compresie ,funcții SSL offloading, precum si protectia aplicatiilor in cazul atacurilor). Folosind soluțiile de tip hardware ADC, infrastructura va funcționa corespunzător și în cazul procesării unui număr mare de tranzacții." a precizat Sergiu Banyai.

Evoluția portofoliului de soluții

Ca o consecință a diversificării atacurilor, discutăm astăzi despre o varietate mare de soluții de securitate și de un nivel tot mai mare de specializare. *"Și în cazul Veracomp, am extins portofoliul de soluții, acesta incluzând soluții de la Fortinet, F5, Extreme Networks, RSA și WhiteHat. Gama de soluții este capabilă să răspundă unor nevoi variate, atât din punctul de vedere al arhitecturii unei infrastructuri, cât și din cel al scalabilității acesteia."* a adăugat Sergiu Banyai.

Evoluția pieței de securitate IT

Piața de securitate IT înregistrează la nivel global una dintre cele mai importante creșteri, tendințele pieței locale fiind diferite. *"Pe piața locală, constatăm existența unor bugete insuficiente pe zona de securitate IT. De asemenea, companiile locale reacționează, în cele mai multe cazuri, după ce au întâmpinat probleme de securitate și au înregistrat pierderi financiare sau de altă natură."* a declarat Sergiu Bayai.

"Lipsa unor acțiuni proactive, în ceea ce privește atacurile cibernetice, poate aduce prejudicii importante pentru companii. Acum câțiva ani, amenințările la nivel de rețea se limitau la atacuri volumetrice brute tip DoS/DdoS, iar cele legate de aplicatii priveau in general modificarea conținutului web-site-urilor sau al bazelor de date suport pentru acestea, aceste modificări fiind realizate de dragul distracției sau din dorința de a experimenta. Astăzi, atacurile direcționate către companii sau utilizatori de internet urmăresc ca scop principal un interes pecuniar.

Ca și exemple, troienii CryptoLocker și CryptoWall criptează fișierele utilizatorilor, solicitând ulterior o sumă de bani pentru primirea cheii de decriptare.

La nivelul infrastructurilor companiilor sau organizațiilor guvernamentale, atacurile se realizează tot mai mult la nivel macro și țintesc de cele mai multe ori informatii critice sau senzitive, fiind coordonate de nuclee foarte bine pregătite sustinute de state sau organizații criminale. În acest context, a investi în soluții de securitate de ultimă generație este o cerință obligatorie pentru organizații." a declarat Sergiu Banyai.

Silviu Cojocaru

4 tendințe în securitatea IT

Sergiu Banyai identifică patru tendințe fundamentale, în ceea ce privește modul de realizare a atacurilor informatice.

1. Atacuri asupra infrastructurii critice a organizațiilor sau instițutiilor guvernamentale, foarte specializate, realizate de grupuri bine pregătite, unele chiar sponsorizate de diverse state sau grupări criminale organizate.

2. Atacurile direcționate către diverse bănci. În acest caz, se observă o evoluție clară a metodelor, de la malware precum Zeus ,Citadel, Conficker, la Dyre si Jbot ce sunt direcționati doar către clienții anumitor bănci și includ mecanisme de evitare a detecției.

3. Exploit-uri din ce in ce mai sofisticate, având ca si țintă sistemele de operare mobile (Android, OS X) și aplicațiile mobile tip open-source. Apple Pay, Google Wallet și aplicatiile bazate pe NFC vor fi unele dintre țintele favorite ale anului 2015.

4. Extinderea așa numitelor „darknets", printre acestea se numărându-se: TOR, Freenet, I2P etc. Acestea vor crea o bază comună de „operațiuni" a diverselor grupări malițioase organizate, în definirea, testarea și implementarea noilor tipuri de atacuri informatice.

O nouă etapă în evoluția companiei Intergraph

A 13–a ediție a evenimentului "Lumea Geospațială" s-a impus ca fiind cel mai important eveniment dedicat comunității geospațiale din România într-o piață IT extrem de dinamică. Cu acest prilej, Aurel Băloi , noul director general, ne-a prezentat câteva dintre elementele noii strategii a companiei Intergraph Computer Services (ICS).

„Ideea de comunitate și crearea unui cadru de colaborare și de împărtășire a experiențelor a fost și continuă să fie cheia succesului <<Lumii Geospațiale>>", ne-a declarat Aurel Băloi.

"Am reușit să construim o comunitate în care se exprimă atât oameni specializați în domeniul IT, cât și experți tehnici și manageri de business din administrații publice, companii de utilități, infrastructuri critice și instituții de ordine și siguranță publică. Prezentări în plen, mese rotunde, ateliere practice, „colțul consultantului, concursuri sunt doar câteva activități care au captat interesul participanților. Din acest an, au fost alocate secțiuni separate domeniilor cercetării și educației. Colaborarea cu mediul academic este o prioritate pentru noi, iar prezența în număr din ce în ce mai mare a reprezentanților universităților demonstrează sinergia creată. Suntem siguri că prin aceasta stimulăm noi oportunități de colaborare pe viitor. În plus, programul educațional, Intergraph University, prin intermediul căruia li se oferă studenților și profesorilor acces la platformele tehnologice Hexagon și Intergraph a devenit o permanență și s-a lărgit cu fiecare an care a trecut."

Ca de obicei, "Colțul consultantului" a atras prin „operațiile pe cord deschis" în care consultanța s-a realizat prin demonstrații live ale soluțiilor din portofoliu. Tot aici, soluțiile Intergraph au fost definitivate prin adăugarea componentelor complementare (hardware, soluții de monitorizare, achiziție și procesare de date, echipamente de măsurare) oferite de partenerii noștri prezenți în standurile expoziționale.

Instituția proactivă – datele și serviciile deschise

"Lumea geospațială" a propus un nou capitol de dezbateri pentru a conștientiza nevoia de proactivitate în sectorul public și evoluțiile necesare pentru a crea acest tip de instituții proactive.

"Instituția proactivă este prioritară pentru Uniunea Europeană, care definește două zone de interes pentru dezvoltarea acestui concept. Prima zonă de interes vizează guvernarea deschisă (open government), fiind orientată spre producerea de date și exploatarea acestora prin servicii și decizii deschise în instituțiile publice. Pe baza conceptului de guver-

„Intergraph are o nouă echipă de management, iar eu sunt exponentul noului val de tineri care s-a alăturat companiei. În prezent, avem peste 40 de angajați și colaboratori, ICS trecând la o nouă etapă de dezvoltare, transformându-se dintr-o companie mică într-o companie de talie medie. " Aurel Băloi

nare deschisă, a doua zonă de interes este crearea unui punct unic de contact în administrația publică. Obiectivele Conferinței au fost conștientizarea importanței acestor două zone de interes și pașii de urmat pentru dezvoltarea guvernării deschise în România. " a declarat Aurel Băloi.

Ecosistemul informațional național

Contribuția la dezvoltarea unui nou ecosistem informațional național este unul dintre obiectivele strategice ale ICS.

"Considerăm că prin crearea unui ecosistem național de informații se poate înregistra o evoluție importantă în dezvoltarea instituțiilor publice. Acest ecosistem se bazează pe doi piloni fundamentali: tehnologiile geospațiale și interoperabilitatea implementată prin standarde de schimb de informații. " a declarat Aurel Băloi.

"Primii pași în construirea acestui ecosistem, am reușit să-i facem în domeniul ordinii și siguranței publice. Astfel, prin proiectele implementate la nivelul Ministerului Afacerilor Interne (MAI), primele standarde de informații au fost implementate în România, iar comunicarea informațiilor a fost standardizată, simplificată și automatizată" a continuat Aurel Băloi.

"ICS consideră că dezvoltarea unui ecosistem informațional național este un element fundamental pentru trecerea instituțiilor guvernamentale într-o nouă etapă de dezvoltare. De asemenea, acest ecosistem este fundamentul tehnologic și instituțional pentru crearea punctului unic de contact, în linie cu evoluția și cerințele internaționale."

Saas - Soluții în cloud pentru instituțiile publice sau pentru companiile de utilități

O altă schimbare importantă în strategia ICS este disponibilitatea soluțiilor Intergraph atât "on premises", cât și ca servicii (SaaS – Software As A Service). În acest context, ICS a creat propriul centru de date în România. Serviciile în cloud ale companiei asigură suveranitatea datelor și implementează un set de politici stricte de securitate atât la nivel informatic, cât și la nivel fizic.

"SaaS este fără îndoială o piață emergentă, dar considerăm că va înregistra în curând creșteri importante. Există în România aproximativ 3200 de autorități administrativ teritoriale și multe companii de utilități de talie medie sau mică, care nu pot investi în infrastructură software și hardware, sau nu-și permit experți care să le administreze, cu toate că au mare nevoie. De aceea soluțiile geospațiale pe care le propunem, în forma software disponibil online pe bază de abonament care înlocuiește investițiile cu cheltuielile, contribuie la crearea unui parteneriat din care cu toții câștigăm." a precizat Aurel Băloi.

O nouă etapă în evoluția Intergraph

"Intergraph are o nouă echipă de management, iar eu sunt exponentul noului val de tineri care s-a alăturat companiei. În prezent, avem peste 40 de angajați și colaboratori, ICS trecând la o nouaă etapă de dezvoltare, transformându-se dintr-o companie mică într-o companie de talie medie. În acest context, a fost necesar să schimbăm procesele interne și modul de interacțiune cu clienții. " a precizat Aurel Băloi.

"Intergraph era cunoscută ca o companie care dezvoltă soluții specializate pentru clienți speciali. Astăzi, încercăm să extindem acest concept astfel încât, alături de soluțiile specializate prin valorificarea cunoștințelor acumulate, să implementăm soluții standard pentru procese standard. Dorim să generalizăm și să reutilizăm în viitoarele implementări cunoștințele dobândite pentru fiecare domeniu de activitate în parte (urbanism, drumuri, spații verzi, etc.). Beneficiile sunt însemnate atât pentru noi, cât și pentru clienții noștri. Implementările se vor realiza însă mai rapid, fără riscuri – soluția putând fi testată înainte de achiziție, cu optimizarea resurselor și cu costuri semnificativ reduse." a concluzionat Aurel Băloi.

Silviu Cojocaru

CUM VOM CĂLĂTORI PÂNĂ ÎN 2030?

Turismul a cunoscut o continuă extindere și diversificare, pentru a deveni unul dintre cele mai mari și cu cea mai rapidă creștere sectoare economice din lume. Un număr tot mai mare de destinații din intreaga lume au devenit destinații turistice, transformându-se într-un factor cheie de progres socio-economic, prin crearea de locuri de muncă, creșterea veniturilor din export, și dezvoltarea infrastructurii. Conform datelor publicate de Organizația Mondială a Turismului (http://www2.unwto.org/), în 2014 au fost înregistrați aprox. 1,4 miliarde de turiști, care au cheltuit 1245 miliarde USD.

Numărul turiștilor va continua să crească; până în 2030, mai mult de 1,8 miliarde de persoane vor călători la nivel internațional, în fiecare an, iar ceea ce îi va motiva și felul cum se vor comporta acești călători ai secolului 21 va fi radical diferit de ceea ce vedem astăzi. Cel puțin, asta spune un studiu recent comandat de Amadeus, lider mondial în furnizarea de soluții de tehnologie și de distribuție pentru industria de turism.

Până la sfârșitul deceniului următor, se estimează că unele persoane vor achiziționa și consuma experiențe de călătorie luând în considerare cât de ușor pot fi distribuite, sau cât de mult „capital" generează, prin intermediul rețelelor sociale. Un alt grup de călători va pune mai presus de orice simplitatea totală și lipsa de efort în a-și organiza călătoriile, apreciind cât mai mult posibil serviciile efectuate la distanță, de către terți. În același timp, un grup important de călători va fi motivat de dorința de a beneficia de experiențele cele mai hedoniste și exclusiviste.

Acestea sunt doar câteva dintre concluziile și previziunile prezentate de *„Future Travel Tribes 2030: understanding tomorrow's travellers"*, un raport comandat de Amadeus și realizat de Future Foundation, ce urmărește înțelegerea diferitelor tipologii de călători ce vor apărea în viitor. Raportul are ca scop, totodată, și identificarea segmentelor din industria de turism ce se așteaptă să se dezvolte sau să ia amploare în următorii 15 ani.

Cum ar trebui să reacționeze furnizorii de servicii de turism la aceste tendințe? Ei bine, aceștia trebuie să țină cont de faptul că modul în care noii clienți achiziționează serviciile și intră în contact cu industria de turism, este pe cale să se schimbe. Vor fi agențiile de turism

Future Travel Tribes 2030

Cercetarea „Future Travel Tribes 2030: understanding tomorrow's travellers", ce a avut o abordare mai degrabă psihologică decât demografică, a condus la identificarea a șase tipuri de personalități distincte de călători, precum:

• **Iubitorii de social media** își vor structura vacanțele ținând cont, aproape permanent, de publicul online. Aceștia se bazează foarte mult pe evaluări și recomandări online pentru a-și valida deciziile de vacanță sau călătorie. Astfel, o piață cu totul nouă se poate deschide pe baza postărilor și opiniilor unor leaderi de opinie cu care interacționează călătorii pe diferitele rețele sociale.

• **Iubitorii de autenticitate culturală** vor vedea vacanțele drept tot atâtea șanse de a lua contact cu alte culturi noi, chiar dacă experiențele nu sunt cele mai confortabile; pentru aceștia, bucuria vacanței depinde în cea mai mare măsură de autenticitatea experienței culturale.

• **Călătorii „etici"** își vor face planuri de călătorie motivați de aspecte morale, precum scăderea emisiilor de carbon sau îmbunătățirea vieții altora. Adesea, ei vor improviza sau vor adăuga elemente de voluntariat, dezvoltarea comunității sau activități ecologice vacanțelor lor.

• **Iubitorii de simplitate** vor prefera pachetele complete de vacanță, căutând să evite administrarea prea multor detalii privind vacanțele sau călătoriile lor. Pentru acest grup de călători, vacanța reprezintă un moment de răsfăț, bucurie, dar și de siguranță și confort.

• **Călătorii "cu scop"** sunt cei care au de obicei un scop specific pentru călătorii, indiferent dacă de afaceri sau de agrement, și, astfel, au constrângeri de timp și buget. Aceștia vor căuta să-și planifice călătoria în cel mai simplu și eficient mod cu putință, adesea bazându-se pe tehnologie.

• **Iubitorii de „recompense"** sunt interesați doar de călătoriile ce oferă experiențe extraordinare. Ei caută oferte spectaculoase, aleg călătorii "must have" și pretind întotdeauna experiențe de vacanță premium, adesea văzute ca un drept câștigat prin investiția de timp și energie la locul de muncă.

cu afișe lipite la stradă de domeniul istoriei, în curînd? Nu știm, dar cu siguranță, dorința călătorilor de a-și împărtăși online experiențele de călătorie va fi profundă, vor apărea noi surse de inspirație pentru noi vacanțe și vor fi influențate și tendințele de cumpărare. Iubitorii de social media, de exemplu, vor căuta inspirație pentru călătoriile lor pe rețelele sociale și vor achiziționa vacanțe recomandate de prieteni. Unele destinații pot deveni „must see" dacă și prietenii virtuali postează despre ele.

Dar și câteva recenzii nefavorabile, postate online, pot avea efect dezastruos. În același timp, potențialii călători se vor aștepta la un grad foarte ridicat de personalizare din partea furnizorilor, aceasta fiind poate a doua mare tendință din domeniu, după „democratizarea" accesului la informație și faptul că experiențele de călătorie, fie ele pozitive sau negative, pot deveni rapid virale pe internet.

Studiul citat arată că potențialii clienți vor pune un accent mult mai mare, în primul rând, pe experiența furnizată, și în al doilea rând, pe etică, atât de mediu cât și cea socială, acestea influențând în mod semnificativ opțiunile de călătorie și comportamentul acestora.

În acest sens, înțelegerea tipologiilor predominante de călători va fi un aspect vital pentru toți furnizorii, cumpărătorii și vânzătorii de servicii de turism în următorii ani. Aceasta poate avea un impact major: de la a ajuta unele deciziile de investiții în noi capacități hoteliere, de exemplu, la concentrarea pe anumite canale de vânzări, și până la adoptarea unor noi tehnologii. Și aici ne referim, în primul rând, la ceea ce numim tehnologia informației.

Prin urmare, un nou studiu recent „**Future Travellers Tribes 2030: Building a more rewarding journey",** comandat de aceeași companie, subliniază felul în care companiile aeriene și furnizorii de servicii turistice complementare pot servi mai bine nevoile de călătorie în viitor, prin strategii mai eficiente de merchandising și implementare de noi soluții IT. Studiul explică, de asemenea, și modul în care călătoriile însele se vor schimba până în 2030, în cea mai mare parte datorită mai bunei folosiri a informațiilor disponibile, a noilor tehnologii și extinderii canalelor de vânzări.

Articolul complet și infogarficul sunt dpsonibile la adresa http://itchannel3.itchannel.ro/?p=15261

SOLUȚIILE AMADEUS - REDUCERI CU 40% PENTRU CĂLĂTORIILE DE AFACERI

Evenimentul "Smart ideas for cost effective business travel budget" (organizat în parteneriat de Weco Travel, Amadeus, Lufthansa Group și AirPlus International) și-a propus să prezinte mai multe soluții prin care companiile își pot optimiza costurile călătoriilor de afaceri.

Amadeus a prezentat soluția eTravel Management (AeTM), soluție care este utilizată în prezent de aproximativ 7.200 de organizații la nivel global, printre acestea regăsindu-se: IKEA, P&G, Orange, Microsoft, SAP, Johnson & Johnson etc.
Robert Komartin, Country Manager, Amadeus Romania a declarat:*"Soluția AeTM poate reduce semnificativ atât timpul alocat operațiunilor de rezervare, cât și costurile călătoriilor de afaceri. Potrivit studiilor realizate de Amadeus printre clienții AeTM, timpul alocat operațiunilor de administrare a călătoriilor poate fi redus cu 80%, iar costurile aferente cu până la 40%."*

Potrivit studiilor realizate de Google (disponibile pe site-ul https://www.thinkwithgoogle.com/) aproximativ 80% dintre călătoriile de afaceri sunt planificate folosind resurse informaționale oferite de Internet, iar dispozitivele mobile sunt

utilizate tot mai frecvent pentru realizarea operațiunilor de rezervare. În acest context, AeTM dispune de o interfață web based, bazată pe conceptul single-page application (SPA), fiind simplu de utilizat pentru procesele de self-booking realizate de angajați. Suplimentar, pot fi stabilite fluxuri de aprobare și politici de travel la nivel de organizație.
"În modelul tradițional de booking, rezervările se realizează via telefon sau e-mail. Procesul de rezervare nu este formalizat, fiind cronofag și presupunând multiple iterații între client și agenția de turism. AeTM simplifică procesul de rezervare și realizează interacțiunea mult mai simplă cu agenția de turism, prin intermediul unui portal web. De asemenea, pot fi implementate politici de călătorie foarte stricte (spre exemplu numai anumite persoane din organizație pot călători la clasa business), acest lucru conducând la reducerea costurilor." a completat Robert Komartin.

AeTM poate fi integrat cu alte sisteme folosite de companii (e.g. soluții financiare sau de tipul Enterprise Resource Planning), contribuind astfel la automatizarea proceselor de afaceri din organizații. Potrivit studiului "Shaping the Future of Travel" , realizat de Oxford Economics și Amadeus, numărul călătoriilor de afaceri va crește seminificativ până în anul 2020. Procesele de gestionare a rezervărilor în companii vor fi tot mai complexe și mai greu de gestionat, în lipsa unor mijloace adecvate. În acest context, soluția propusă de Amadeus poate optimiza aceste procese de rezervare și poate aduce beneficii importante organizațiilor.

Industria de Software și Servicii IT - peste 2,4 miliarde EUR în 2014

Veniturile companiilor românești de software și servicii IT au crescut cu 13% în 2014 față de 2013, ajungând la 2,42 miliarde euro, conform Studiului „Software and IT Services in Romania", făcut public astăzi de către ANIS - Asociația Patronală a Industriei de Software și Servicii și realizat de către PAC - Pierre Audoin Consultants.

Prognoza pentru 2015 indică o creștere de 14% a veniturilor industriei, iar rata de creștere anuală medie estimată pentru următorii 3 ani este de 11%.

Din totalul veniturilor, aproximativ 65% au provenit în 2014 din exporturi, în creștere față de anul anterior când ponderea exporturilor în veniturile din software și servicii ale companiilor românești era de 60% (informații suplimentare sunt disponibile în graficul de mai jos, care prezintă evoluția pieței în cifre absolute, precum și ratele de creștere).

"Industria de software și servicii este una dintre cele mai performante pe care România le are în prezent, dată fiind rata de creștere de 4 ori mai mare decât cea estimată pentru întreaga economie. În 2014, industria IT&C a înregistrat cea mai mare pondere în PIB de până acum - 6%, din care 2,5% este generat de software și servicii. Studiul efectuat de către partenerii de la PAC ne arată că tendințele de creștere, mai ales la export, sunt solide și nu sunt bazate pe oportunități trecătoare", explică Teodor Blidăruș (foto), Vicepreședinte ANIS.

"Industria de software și servicii informatice din România are astăzi o singură barieră foarte solidă care o împiedică să crească în continuare cu peste 15-20% pe an: numărul și gradul de pregătire a specialiștilor. România se află astăzi în fața unei șanse uriașe de a deveni un motor regional pentru servicii IT și produse software, cu condiția ca sistemul de educație să evolueze rapid, iar facilitățile fiscale să ajute la crearea de valoare adăugată. Potențialul teoretic al industriei de software și servicii informatice este de peste 6 miliarde de euro până în 2020, însă acest nivel nu se va atinge într-un mod haotic, ci doar într-un cadru extrem de organizat, de la nivel de sistem educațional, curriculum, facilități fiscale, fonduri europene folosite corect și atragere de investiții masive.", explică Eugen Schwab, Vice-President Romania & CEE în cadrul Pierre Audoin Consultants (PAC).

Veniturile realizate de companiile românești în țară provin în proporție de 32% din proiecte derulate pentru administrația publică, 16% pentru clienți din industria producătoare, 14% pentru clienți din zona financiar-bancară, 9% pentru companii telecom și 8% pentru clienți din domeniul utilităților. La export, veniturile provin de la clienți din industria producătoare în proporție de 40%, 17% de la clienți din domeniul serviciilor, 16% din zona financiar-bancară, 11% din retail și 5% din asigurări.

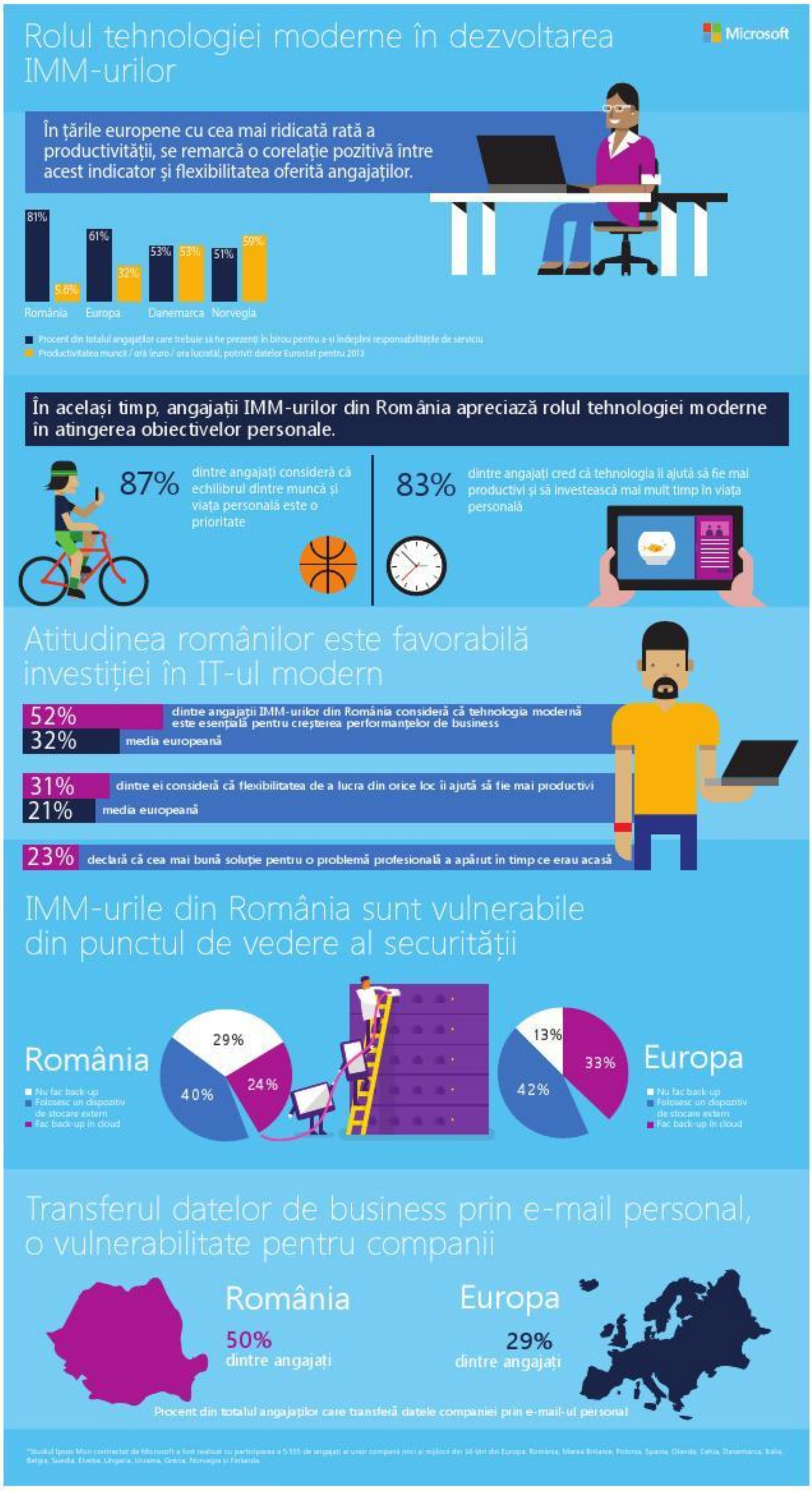
INTEGRAREA TEHNOLOGIILOR MOBILE ÎN CADRUL IMM-URILOR

Conform unui studiu Ipsos MORI realizat pentru Microsoft în Europa, angajații IMM-urilor din România continuă să creadă în tehnologia mobilă și în îmbunătățirea relației cu clienții, ca principale motoare pentru creșterea perfomanțelor companiilor.

Un studiu Ipsos Mori realizat pentru Microsoft în anul 2015 arată că România este țara europeană cu cel mai mare număr de angajați nevoiți să fie prezenți la birou pentru a-și îndeplini sarcinile de lucru (81%), la polul opus aflându-se Norvegia, unde doar 51% dintre angajații IMM-urilor trebuie să fie prezenți la birou. În același timp, datele Eurostat arată că rata productivității în România era de 5,6 euro / oră în 2013, adică de șase ori sub media europeană și de aproape 12 ori mai mică decât rata productivității în Norvegia (59 euro / oră). Rezultatele sugerează o corelație pozitivă între gradul de receptivitate la integrarea tehnologiilor mobile în mediul de lucru și productivitatea angajaților din economie.

Același studiu Ipso Mori arată că peste jumătate dintre angajații români (52%) consideră că investiția în IT reprezintă o prioritate pentru creșterea performanțelor de business, iar 50% dintre ei consideră că o relație mai bună cu clienții ar putea avea același rezultat. Cercetarea a fost realizată în 16 țări din Europa, printre care și România, cu participarea a 5.555 de angajați din companii mici și mijlocii.

În România, mai mult decât în orice altă țară participantă la studiu, angajații IMM-urilor pun preț pe echilibrul dintre muncă și viața personală. Acesta este o prioritate pentru 87% dintre ei, spre deosebire de media europeană de 73%. Pentru a-și atinge acest obiectiv, cei mai mulți dintre angajații români, respectiv 83%, consideră că tehnologia mobilă i-ar putea ajuta să fie mai productivi și să întrețină echilibrul dintre planul profesional și cel privat.



Articolul complet este disponibil pe site-ul http://itchannel3.itchannel.ro/?p=14938

Open Source pe Microsoft Azure

Încă de la lansarea platformei în cloud Azure, Microsoft a fost interesată să ofere suport pentru aplicațiile open source. În prezent, 20% dintre aplicațiile găzduite pe platformă sunt mașini virtuale cu Linux. În acest context, Microsoft a organizat un workshop dedicat comunității de administratori și dezvoltatori pentru platformele open source,

"Compania noastră a depus un efort continuu în susținerea comunității open source, iar rezultatele se văd în cifrele legate de Microsoft și open source. Evenimentul face parte dintr-o serie de workshop-uri organizate de Microsoft la nivel regional. Workshop-urile sunt orientate spre zona practică, având ca principal scop prezentarea unor instrumente de migrare pe Microsoft Azure și a avantajelor acestei platforme." a precizat Marius Filipaș, Cloud&Enterprise Lead Microsoft.

Microsoft a avut o contribuție importantă la dezvoltarea kernelului Linux, peste 20.000 de linii de cod fiind adăugate de companie. Numărul de aplicații, disponibile în modalitatea open source, pe platforma Codeplex a crescut de la 300.000 în 2010 la peste 1 milion în 2014. De asemenea, implementările de mașini virtuale cu Linux pe Microsoft Azure reprezintă 20% din totalul implementărilor.

"Azure aduce ca principal avantaj viteza cu care sunt publicate mașini virtuale cu Linux pe platformă. Pot fi create soluții complexe pe platforma de cloud, asamblând diverse componente în mod asemănător cu piesele Lego.

De asemenea, există diverse distribuții Linux și aplicații open source (Wordpress, Drupal, Magento etc.) pentru care configurarea pe platforma Azure este în totalitate automatizată. Acest lucru conduce la reducerea substanțială a timpului în care diverse soluții Linux și open source devin operaționale pe platforma open source." a precizat Michal Smereczynski (CEO – Free media). Michal este evanghelist al interoperabilității dintre soluțiile Microsoft si Open Source Software, în cadrul workshop-ului realizând mai multe prezentări tehnice.

"Printre avantajele platformei Azure se numără suportul oferit în procesele de migrare și întreținere a platformelor open source și Linux. De asemenea, costurile platformei Azure sunt sensibil mai mici în comparație cu alte platforme de pe piață. " a precizat Ryszard Dalkowski, Consultant – Exertum.

Din noiembrie 2014, .NET Framework – unul dintre cele mai importante proiecte Microsoft – a devenit un proiect open source, comunitatea fiind găzduită de site-ul http://www.dotnetfoundation.org/ .

Pe lângă limbajele specifice platformei .NET, programatorii pot scrie cod în Java, Node.js, PHP, Python și Ruby. Platforma Azure oferă suportul pentru numeroase distribuții Linux, printre acestea numărându-se: Canonical, CoreOS, OpenLogic, Oracle și SUSE.

Suportul Microsoft pentru comunitatea open-source în cifre

20% din mașinile virtuale pe Azure cu Linux

1.000.000 de aplicații publicate pe CodePlex

20,000 de linii de cod contribuția Microsoft la kernelul Linux

Test - Allview Wi10N PRO

Wi10N PRO este o tabletă cu Windows 8.1 cu facilități foarte bune, modelul fiind dotat și cu tastatură. La prima vedere te impresionează calitatea carcasei și a materialelor utilizate.

Cu toate că nu dispune de o carcasă de aluminiu, materialele folosite la exterior sunt de calitate și dau senzația de durabilitate. Îmbinarea dintre tabletă și tastatură este foarte simplă și pare a asigura garanția fiabilității pe termen lung, scoaterea tabletei din portul tastaturii fiind unul dintre testele de anduranță pentru astfel de modele hibride.

Procesul Quad Core are performanțe foarte bune atât pentru Office, cât și pentru jocuri. De asemenea, dispozitivul dispune 2 GB memorie RAM, 32 GB memorie Flash, un display de 10,1 inch (rezoluție 1280x800 pixeli). La capitolul porturi se regăsesc: două porturi USB (unul pe tastatură și unul pe tabletă), un port micro HDMI, jack audio de 3,5 mm și cititor pentru memorie microSD cu care poate fi extinsă memoria cu până la 32 GB.

Consider că Wi10N este un "laptop replacement" foarte util pentru cei care călătoresc și au nevoie de un dispozitiv foarte ușor pe care să lucreze la fel de eficient ca pe un notebook. Greutatea de 1,1 kg împreună cu tastatura (630 g numai tableta) fac din Wi10N un dispozitiv ultra-portabil.

Wi10N include o serie de alte funcționalități, care sunt rezultatul parteneriatului dintre Microsoft și Allview. Printre acestea se numără: licența pentru Windows 8.1, abonament pe un an la Office 365 Home Edition (abonamentul include atât aplicațiile Web, cât și aplicațiile desktop cele mai utilizate-Word, Excel, PowerPoint), OneDrive cu spațiu de 1 TB.

Pe scurt

•Un raport excelent preț/performanță (prețul, potrivit Allview la data redactării articolului, a fost de 1099 RON)
•Dispozitiv ultra-portabil (1,1 Kg tableta împreună cu tastatura)
www.allview.ro

Windows Server 2003- încheierea suportului tehnic

Microsoft anunță încheierea perioadei de suport tehnic pentru Windows Server 2003, fără posibilitate de prelungire. Această dată este conformă procedurilor standard de asistență pe parcursul ciclului de viață al produsului - cinci ani de zile suport de bază și încă cinci ani suport extins. Migrarea de la Windows Server 2003 către Windows Server 2012 R2 le oferă clienților oportunitatea de a-și îmbunătăți infrastructura și performanțele aplicațiilor pe care le rulează, prin creșterea nivelului de siguranță, cu impact pozitiv asupra satisfacției clienților.

În România, Microsoft estimează că 25% dintre companii (dintre care preponderent IMM-uri) rulează încă tehnologia Windows Server 2003. Aceste companii se expun unor riscuri ridicate de securitate și lipsă de compliance.

Un singur server neasistat cu patch-uri implică riscuri pentru întreaga infrastructură a unei companii, iar virtualizarea sau utilizarea acestora în cloud nu elimină riscurile de securitate.

Organizațiile care vor rula Windows Server 2003 după 14 iulie 2015 se vor expune următoarelor riscuri:

•**Lipsa actualizărilor** - nu mai puțin de 37 de actualizări esențiale au fost lansate în 2013 pentru Windows Server 2003/R2 în cadrul extinderii perioadei de suport.

•**Lipsa conformității** - Respectarea reglementărilor legale și a standardelor din domeniu sunt esențiale pentru o gamă largă de companii. Utilizarea unor produse în afara perioadei de suport aduce cu sine posibile penalități și tarife tranzacționale mari rezultate din lipsa conformității cu diverse standarde și reglementări.

•**Lipsa protecției datelor** - Atât instanțele fizice, cât și instanțele virtualizate de Windows Server 2003 sunt vulnerabile și nu ar trece de un audit. Chiar dacă o aplicație este securizată și conformă cu cele mai recente standarde de siguranță, rularea ei pe Windows Server 2003 o transformă într-o aplicație neconformă.

•**Costuri suplimentare** - Un acord de asistență particularizat are un cost foarte ridicat, iar clienții trebuie să plătească în plus pentru sisteme de securitate, firewall-uri avansate și alte măsuri de securitate - doar pentru a izola serverele cu sistem de operare Windows Server 2003.

Internet Security Threat Report - cinci din șase companii mari au fost vizate în 2014

În lumea conectată de astăzi, nu se mai pune problema dacă vei fi atacat, ci când. Raportul Symantec cu privire la ameninţările de securitate online Internet Security Threat Report (ISTR), „Volumul 20", expune o schimbare de tactică a atacatorilor cibernetici: se infiltrează în reţele şi evită detectarea, atacând infrastructura corporaţiilor importante şi folosind-o împotriva acestora.

"*Atacatorii nu au nevoie să spargă uşa către reţeaua unei companii, din moment ce cheile de acces sunt deja disponibile*", a afirmat Kevin Haley, director Symantec Security Response. " *Vedem cum atacatorii determină companiile să se infecteze prin trimiterea de troieni în actualizările de software ale programelor obişnuite, după care aşteaptă răbdători ca ţintele să le descarce, oferind astfel atacatorilor acces liber la reţeaua corporației.*"

Raportul Symantec arată că cinci din şase companii mari au fost vizate în 2014, o creştere de 40% faţă de anul precedent. În 2014 au existat în total 24 de vulnerabilităţi de tip zero-day, lăsând câmp deschis atacatorilor pentru exploatarea breşelor cunoscute înainte de aplicarea patch-urilor.

Atacatorii reuşesc cu viteză şi precizie

Într-un an record în ceea ce priveşte vulnerabilităţile de tip zero-day, cercetarea Symantec dezvăluie faptul că pentru crearea şi dezvoltarea de patch-uri, companiile de software au avut nevoie în medie de 59 de zile, comparativ cu numai patru zile în anul 2013. Atacatorii au profitat de întârziere şi, în cazul Heartbleed, s-au grăbit să exploateze vulnerabilitatea într-un interval de patru ore. În 2014 au existat în total 24 de vulnerabilităţi de tip zero-day, lăsând câmp deschis atacatorilor pentru exploatarea breşelor cunoscute înainte de aplicarea patch-urilor.

Între timp, atacatorii avansaţi au continuat să pătrundă în reţele cu atacuri de spear-phishing bine direcţionate, ceea ce a dus la o creştere totală de 8% în 2014. O particularitate a fost precizia atacurilor de anul trecut, care au folosit cu 20% mai puţine email-uri pentru a-şi atinge ţintele şi au încorporat mai multe atacuri de tip drive-by download şi alte exploatări web.

În plus, Symantec a observat că atacatorii:

- Au folosit conturi de email furate de la o victimă corporatistă în vederea atacurilor de spear-phishing către alte victime situate mai sus pe scara ierarhică;
- Au folosit instrumentele şi procedurile de management ale companiilor pentru a muta IP-ul furat în jurul reţelei corporatiste înainte de exfiltrare;
- Au construit software-uri de atac specifice în reţeaua victimelor pentru a-şi camufla activităţile.

Extorsiunea informatică este în creştere

Email-ul rămâne un vector de atac semnificativ pentru infractorii cibernetici, însă aceştia continuă să experimenteze noi metode de atac pe dispozitivele mobile şi reţelele sociale, pentru a ajunge la mai mulţi oameni cu mai puţin efort.

"Infractorii cibernetici sunt leneşi din fire; ei preferă să-şi desfăşoare activităţile murdare cu instrumente automatizate şi cu ajutorul consumatorilor neavizaţi", a adăugat Kevin Haley, director Symantec Security Response. *"Anul trecut, 70% dintre escrocheriile din reţelele sociale s-au răspândit manual, pentru că atacatorii au profitat de disponibilitatea oamenilor de a avea încredere în conţinutul distribuit de prieteni."*

În timp ce escrocheriile din reţelele sociale le pot furniza rapid bani infractorilor cibernetici, unii se bazează pe metode de atac mai avantajoase şi mai agresive, precum ransomware, care anul trecut a avut o creştere de 113%. Astfel, au existat de 45 de ori mai multe victime ale atacurilor crypto-ransomware anul trecut comparativ cu 2013.

În loc să pretindă a aplica legea căutând să amendeze conţinuturi furate, aşa cum am observat în cazurile obişnuite de ransomware, un stil mai vicios de atac crypto-ransomware preia fişierele, fotografiile şi alte conţinuturi digitale ale victimei, fără a masca intenţia atacatorului.

Securizaţi prin diverse metode

Pe măsură ce atacatorii persistă şi evoluează, există mai mulţi paşi pe care companiile şi utilizatorii îi pot face pentru a se proteja. Pentru început, Symantec recomandă următoarele practici ca fiind optime:

Pentru companii:

- Fiţi pregătiţi: Folosiţi soluţii avansate împotriva ameninţării cunoscute, pentru a găsi mai uşor indicatorii de compromitere şi pentru a răspunde mai rapid la incidente.

- Folosiţi un sistem de securitate puternic: Implementaţi solutii de securitate la nivele multiple, endpoint, securitate de reţea, criptare, autentificare puternică şi tehnologii

de prestigiu. Colaboraţi cu un furnizor de servicii de securitate pentru a vă extinde echipa IT.

• Pregătiţi-vă pentru ce e mai rău: Datorită managementului incidentelor, cadrul dumneavoastră de securitate este optimizat, măsurabil şi repetabil, iar lecţiile învăţate vă îmbunătăţesc postura de securitate. Luaţi în considerare includerea unei asistenţe din partea unei terţepărţi, care să vă ajute în gestionarea situaţiilor de criză.

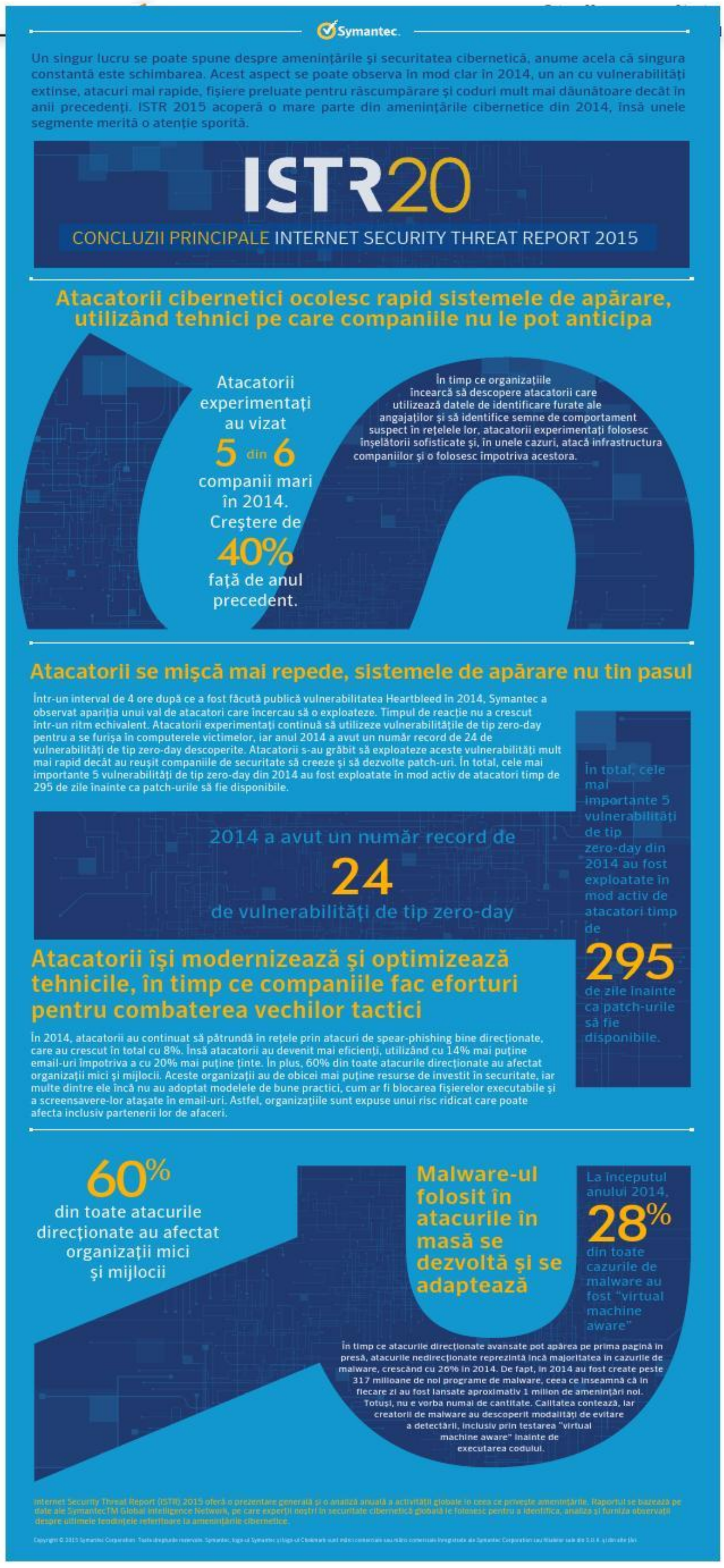
• Asiguraţi educaţie şi instruire permanentă: Stabiliţi ghiduri, politici şi proceduri ale companiei pentru protejarea datelor de pe dispozitivele personale şi corporatiste. Stabiliţi în mod regulat echipe de investigaţie internă şi desfăşuraţi exerciţii practice pentru a vă asigura că aveţi abilităţile necesare pentru combaterea eficientă a ameninţărilor cibernetice.

Pentru utilizatori:

• Folosiţi parole puternice: Acest aspect este extrem de important. Folosiţi parole puternice şi unice pentru conturile şi dispozitivele dumneavoastră şi actualizaţi-le în mod regulat - ideal ar fi la fiecare trei luni. Nu folosiţi niciodată aceeaşi parolă pentru mai multe conturi.

• Fiţi precauţi în reţelele sociale: Nu faceţi clic pe link-uri din email-uri nesolicitate sau din mesaje distribuite prin reţelele sociale, în special din surse necunoscute. Escrocii ştiu că oamenii sunt mai tentaţi să acceseze link-uri de la prieteni şi, de aceea, compromit conturi pentru a trimite link-uri dăunătoare către contactele celui care deţine contul.

• Fiţi atenţi la partajare: Atunci când instalaţi un dispozitiv conectat la reţea, cum ar fi un router, sau atunci când descărcaţi o aplicaţie nouă, verificaţi permisiunile pentru a vedea ce date oferiţi. Dezactivaţi accesul de la distanţă atunci când acesta nu este necesar.



Managementul Crizelor

Pe parcursul săptămânii în care închideam numărul curent al revistei, un grup de hackeri a preluat pentru o scurtă perioadă controlul asupra rachetelor Patriot staționate în Turcia. De asemenea, bursa de pe Wall Street a avut una dintre cele mai mari perioade în care nu a funcționat, se pare în urma unui atac a cunoscutului grup de hackeri Anonymous.

În acest context și într-un număr dedicat securității IT, considerăm că prezentarea unui master dedicat Managementului Crizelor este foarte utilă. Am discutat cu Prof. Univ Dr. Marian Zulean (coordonatorul acestui program de studii) despre acest master și vă prezentăm principalele coordonate ale acestuia.

Masterul este organizat de Facultatea de Administrație și Afaceri, din cadrul Universității din București. Programul "Managementul crizelor" reprezintă o structură de master ce asigură certificări specifice atât administrației publice, cât și mediului privat.

"Masterul <<Managementul crizelor>> își propune să formeze competențele necesare pentru înțelegerea, prevenirea și managementul crizelor. Misiunea acestui program de master este de a forma, în concordanță cu standardele de calitate recunoscute ale Universității din București, specialiști în prevenirea și gestionarea crizelor, analiza și valorificarea informațiilor și managementul proiectelor, care să contribuie la îmbunătățirea sistemului economic și la creșterea organizațiilor publice și private naționale și europene." a precizat Marian Zulean.

Printre obiectivele programului se numără:

- Formarea de specialiști de înaltă calificare în prevenirea și gestionarea crizelor;
- Asigurarea competențelor necesare în domeniu medierii și gestionării conflictelor;
- Asigurarea competențelor pentru domeniile de analiză a informațiilor și de coordonare a implementării planurilor operaționale;
- Calificarea în domeniul managementului programelor și proiectelor;
- Integrarea rapidă a componentei teoretice parcurse în stagii aplicative de practică în managementul crizelor (practică în instituții strategice în managementul crizelor, organizații lider în acest domeniu etc.);
- Dezvoltarea activităților de cercetare științifică în domeniul crizelor și conflictelor la nivel național și european.

Orientare spre zona practică

Masterul se bucură de suportul unor cadre didactice cu mare experiență din cadrul Facultății de Administrație și Afaceri (Prof.univ.dr. Ion Bucur, Prof.univ.dr. Constantin Ghiga, Prof.Univ.Dr. Marian Zulean, Conf. univ.Dr. Răzvan Papuc – decanul facultății).

De asemenea, important de subliniat este orientarea masterului spre zona practică. Printre profesorii asociați se numără:

- Dr. Adrian Baciu, președintele Asociației profesionale a companiilor de securitate
- Aurel Băloi, Director General Intergraph Computer Services
- Gen. (rez) dr. Constantin Degeratu, fost șef al Statului Major al Armatei, fost consilier prezidențial și fondator al Institutului de Studii de Securitate
- Claudiu Degeratu, fost director general, MapN, președinte al Comitetului Director CENCOOP și al Comitetului Director al SHIRBRIG
- Chestor de poliție Andrei Gheorghe, Director General Adjunct, Direcţia Generală Management Operaţional
- Gen. (rez) dr. Constantin Degeratu, fost șef al Statului Major al Armatei, fost consilier prezidențial și fondator al Institutului de Studii de Securitate.

MINITAB - SIMPLITATE ÎN PROCESELE DE ANALIZĂ A DATELOR

Noile interfețe grafice și tehnologii integrate în aplicațiile software au redus substanțial timpul necesar pentru învățarea modului de utilizare al acestor aplicații. Minitab este un exemplu de software statistic complex, care prezintă o curbă de învățare foarte rapidă.

Romsym Data, distribuitorul Minitab în România, a organizat un workshop dedicat acestei soluții. Cu prilejul acestui eveniment, am avut ocazia să stau de vorbă cu Sandeep Girn (Academic & Channel Market Specialist la Minitab).

Minitab este un software statistic creat de cercetători de la Pennsylvania State University. Aplicația are mai bine de 4 decenii, prima versiune a aplicației fiind lansată în 1972. Născută în mediul academic, aplicația este, încă, la ora actuală, una dintre cele mai folosite aplicații la disciplinele de statistică în mediul universitar din SUA.

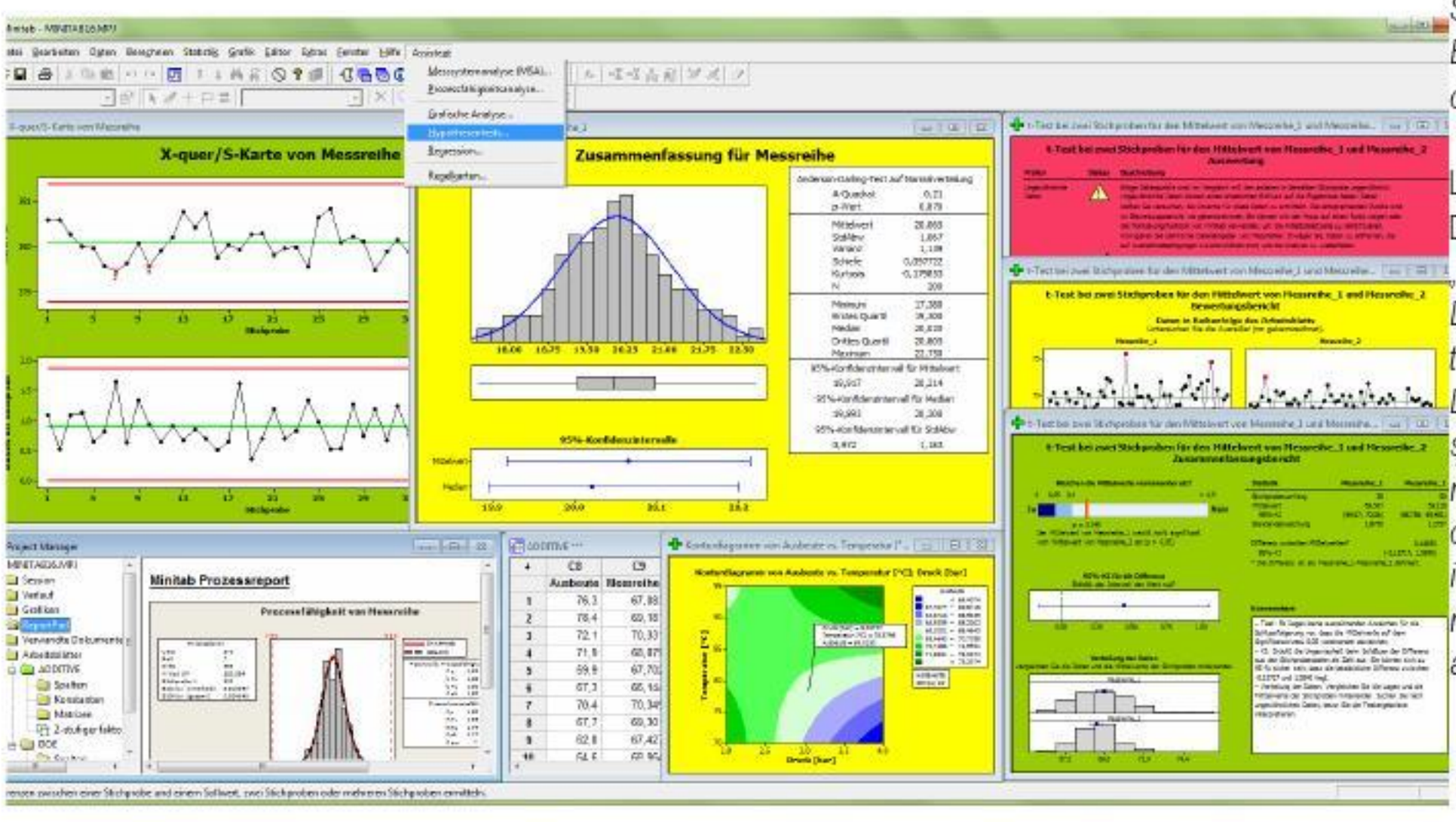
„Pe lângă mediul academic, astăzi Minitab este utilizat în cele mai diverse domenii: industria auto, industria farmaceutică, companii de servicii etc. Suntem prezenți în toate domeniile unde există date de analizat. Spre exemplu, Minitab Quality Companion are o cotă de piață însemnată pe zona de aplicare a algoritmilor statistici în controlul calității (inclusiv pe zona Six Sigma).” a precizat Sandeep Girn.

Minitab oferă și Quality Trainer, o soluție de eLearning care prezintă conceptele statistice specialiștilor în controlul calității, fiind un util instrument de învățare care oferă acces la un mix de cunoștințe legate de Minitab și elemente de statistică.

Minitab a ajuns la versiunea cu numărul 17, care integrează un număr mare de modele statistice și instrumente de reprezentare grafică. Printre acestea se numără: Anova, regresia, modelul Monte Carlo etc. Produsul este însoțit de o interfață simplă, datele statistice fiind exploatate la fel ca în soluțiile de calcul tabelar (datele sunt stocate în foi de calcul, similare cu cele din Excel). Suplimentar, cele mai multe funcții statistice sunt accesibile direct prin intermediul meniului aplicației, fără a folosi comenzi criptice sau limbaje complexe.

Licențiere

Compania Minitab oferă și un model flexibil de licențiere, după cum ne-a declarat Sandeep Girn *„Pe lângă modelul de licențiere perpetuu, Minitab oferă și o modalitate de licențiere bazată pe abonament semestrial sau anual. Versiunea pe bază de abonament este foarte flexibilă, numărul de licențe fiind suplimentat foarte rapid. Dacă ai 10 licențe și peste 3 luni decizi să cumperi încă 10, vei fi taxat numai pentru licențele suplimentare. Modelul de licențiere pentru mediul academic oferă prețuri foarte mici. Spre exemplu, licențele de Minitab Express pot fi închiriate la un preț de sub 50 de EUR anual.”*



Legat de colaborarea cu Romsym Data, Sandeep Girn a declarat: *„Lucrăm îndeaproape cu Romsym Data pentru a livra serviciile noastre pe piața din România. Romsym Data cunoaște utilizatorii locali și ne bazăm pe ei să ne ajute să ne dezvoltăm în această zonă. Ei dețin cunoștințe tehnice și, cel mai important, pot oferi suport în limba nativă, cea ce reprezintă un mare avantaj.”*

Arie van Bennekum – Despre Agile și Kanban

Arie van Bennekum, unul dintre co-autorii Agile Manifesto, a realizat un interesant training la București dedicat Agile și Kanban Am vorbit cu Arie van Bennekum despre Agile și Kanban, precum și despre evoluția acestor concepte. Concluziile discuției sunt disponibile în continuare.

ITCHANNEL: Aș vrea vorbim puțin despre Agile Manifesto pentru că se împlinesc 14 ani de când a fost creat acest concept, acest mod de gândire. Care a fost evoluția acestui concept?

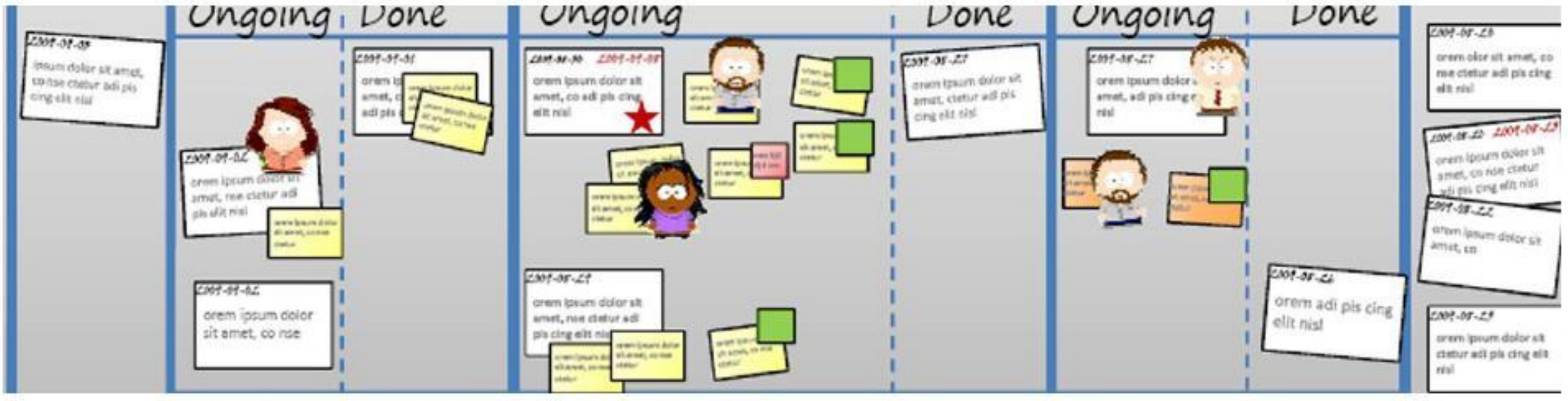
Arie van Bennekum: Cred că sunt multe de spus. Am început să lucrez la dezvoltarea acestui model în 1994, iar în toți acești ani după Agile Manifesto am încercat să instruiesc clienţii pentru îmbunătăţirea continuă a muncii. Diferenţa față de perioada de început, este că vezi din ce în ce mai mulţi oameni integrându-se în sistemul Agile. Cred că astăzi, dacă eşti o organizaţie inteligentă, alegi metodele Agile care te vor ajuta să menții aceleași principii, valori și beneficii în dezvoltarea de soluții. În acest sens, vorbim din ce în ce mai mult despre ansamblarea acestor metode.

ITCHANNEL: Să vorbim și despre Kanban, model care a apărut în industria auto. Care sunt beneficiile pe care le aduce pentru dezvoltarea de software?

Arie van Bennekum: Modelul Kanban oferă multiple avantaje în dezvoltarea de software. Dacă într-o fabrică, principiile Kanban ajută la controlul fluxurilor de lucru, Kanban aplicat în dezvoltarea de software, permite creșterea eficienței echipelor IT folosind concepte precum "Limit Work in Progress" și "Continuous Improvement".

ITCHANNEL: A existat o mutare spre zona de mobilitate. Se observă o schimbare în utilizarea Agile?

Arie van Bennekum: Ceea ce știu este că utilizatorii finali sunt expuși la din ce în ce mai multă informație. Totul este inteligent, astfel că ei cunosc mai multe lucruri despre posibilitățile reale. Dacă ne uităm în întreaga lume, comunitățile de utilizatori finali s-au înmulțit considerabil datorită dispozitivelor mobile; oamenii au acces la aplicații și pot dezvolta la rândul



ITCHANNEL: Aș vrea vorbim puțin despre Agile Manifesto pentru că se împlinesc 14 ani de când a fost creat acest concept, acest mod de gândire. Care a fost evoluția acestui concept?

Arie van Bennekum: Cred că sunt multe de spus. Am început să lucrez la dezvoltarea acestui model în 1994, iar în toți acești ani după Agile Manifesto am încercat să instruiesc clienţii pentru îmbunătăţirea continuă a muncii. Diferenţa față de perioada de început, este că vezi din ce în ce mai mulţi oameni integrându-se în sistemul Agile. Cred că astăzi, dacă eşti o organizaţie inteligentă, alegi metodele Agile care te vor ajuta să menții aceleași principii, valori și beneficii în dezvoltarea de soluții. În acest sens, vorbim din ce în ce mai mult despre ansamblarea acestor metode.

„Cred că Agile tinde să devină un mod de a fi. Este greu de presupus că mai putem proiecta și defini astăzi o soluție complexă fără a aplica principiile Agile.”

Arie van Bennekum

ITCHANNEL: Să vorbim și despre Kanban, model care a apărut în industria auto. Care sunt beneficiile pe care le aduce pentru dezvoltarea de software?

Arie van Bennekum: Modelul Kanban oferă multiple avantaje în dezvoltarea de software. Dacă într-o fabrică, principiile Kanban ajută la controlul fluxurilor de lucru, Kanban aplicat în dezvoltarea de software, permite creșterea eficienței echipelor IT folosind concepte precum “Limit Work in Progress” și “Continuous Improvement”.

ITCHANNEL: A existat o mutare spre zona de mobilitate. Se observă o schimbare în utilizarea Agile?

Arie van Bennekum: Ceea ce știu este că utilizatorii finali sunt expuși la din ce în ce mai multă informație. Totul este inteligent, astfel că ei cunosc

Cele 12 principii ale lui Agile Manifesto

1. Prioritatea noastră este satisfacţia clientului prin livrarea rapidă şi continuă de software valoros.

2. Schimbarea cerinţelor este binevenită chiar şi într-o fază avansată a dezvoltării. Procesele agile valorifică schimbarea în avantajul competitiv al clientului.

3. Livrarea de software funcţional se face frecvent, de preferinţă la intervale de timp cât mai mici, de la câteva săptămâni la câteva luni.

4. Oamenii de afaceri şi dezvoltatorii trebuie să colaboreze zilnic pe parcursul proiectului.

5. Construieşte proiecte în jurul oamenilor motivaţi.Oferă-le mediul propice şi suportul necesar şi ai încredere că obiectivele vor fi atinse.

6. Cea mai eficientă metodă de a transmite informaţii înspre şi în interiorul echipei de dezvoltare este comunicarea faţă în faţă.

7. Software funcţional este principala măsură a progresului.

8. Procesele agile promovează dezvoltarea durabilă.Sponsorii, dezvoltatorii şi utilizatorii trebuie să poată menţine un ritm constant pe termen nedefinit.

9. Atenţia continuă pentru excelenţă tehnică şi design bun îmbunătăţeşte agilitatea.

10. Simplitatea în proiecte este esenţială.

11. Cele mai bune arhitecturi, cerinţe şi design se nasc din echipe bine închegate.

12. La intervale regulate, echipa reflectă la cum să devină mai eficientă, apoi îşi adaptează şi ajustează comportamentul în consecinţă.

NOUA STRATEGIE SYMANTEC

În cadrul unui eveniment dedicat partenerilor din România, Symantec a anunțat strategia legată de separarea business-ului de securitate (tradițional pentru compania Symantec) de soluțiile Veritas (data storage și recuperare de date). La eveniment au participat Vasile Aniculăesei (noul Teritory Manager pentru Veritas) și László György (Territory Manager pentru Symantec).

Symantec este una dintre companiile pioniere în domeniul securității IT, fiind înființată în anul 1982. Symantec a achiziționat business-ul Veritas în anul 2005, valoarea estimată a achiziției fiind la data respectivă de 13,5 miliarde USD. Legat de separarea celor două linii de business și de relația cu partenerii locali, Vasile Aniculăesei (în fotografie) a declarat: *"Nu vor fi schimbări majore pentru partenerii din România. Chiar dacă începând cu luna octombrie va fi realizată o separare juridică a celor două entități, vom colabora în continuare foarte strâns pe toate fronturile (vânzări, marketing, cercetare – dezvoltare etc.) "*

Produsele Veritas sunt lider de piață în categoria de data storage și de recuperare de date. Potrivit informațiilor publicate de Symantec, 75% dintre companiile din Top Fortune folosesc aceste soluții. Gama de produse Veritas include: soluții de backup și restaurare, soluții de storage management și clustering, disaster recovery, arhivare și eDiscovery. Veniturile pentru soluțiile Veritas au însumat 2,5 miliarde USD din totalul veniturilor companiei Symantec, în anul fiscal 2014.

Separarea celor două linii de produse aduce și o noutate pentru piața locală. Vasile Aniculăesei (Teritory Manager pentru Veritas) va coordona o regiune extinsă, care include: România, Bulgaria, Grecia și Cipru. Coordonarea din România a unor țări precum Grecia sau Cipru (fără îndoială mai dezvoltate din punct de vedere IT și economic) este un lucru îmbucurător și, totodată, un plus de încredere acordat managementului local.

76 de achiziții

Potrivit site-ului Symantec, compania a realizat de-a lungul timpului nu mai puțin de 76 de achiziții de companii. Aceasta este însă prima separare a portofoliului de soluții Symantec.
Veritas a fost cea mai scumpă achiziție (13,5 miliare USD). Pe locul 2 se află la mare distanță achiziția Verisign Security Business (1,28 miliarde USD), iar pe locul 3 se regăsește Altiris (1,038 miliarde USD).
Prima achiziție datează din anul 1990 și este vorba de producătoarea faimoasei soluții de securitate și administrare PC Peter Norton (compania Peter Norton a fost achiziționată în anul 1990 pentru 70 milioane USD).

În ceea ce privește business-ul de securitate al Symantec, László György a prezentat, în cadrul aceluiași eveniment, un roadmap al lansărilor de soluții de securitate. Domnul György a reiterat faptul că există în continuare o orientare fermă a companiei pentru a oferi funcționalități care să răspundă nevoilor de securitate pe zona de cloud și virtualizare. De asemenea, au fost prezentate noile configurații de soluții integrate, capabile să răspundă unei palete tot mai vaste de amenințări.

SUNTEM ATÂT DE FERICIȚI

ÎNCAT NE-AM DORIT CA ȘI ACEASTA RECLAMA SA FIE LA FEL

Cea mai mare și complexă implementare de Microsoft Exchange și de Office 365 din România, cel mai bun partener Cloud Public Microsoft din țară în 2011 și 2012 sunt doar câteva motive de bucurie. Restul realizărilor de care suntem mândri, precum și serviciile pe care vi le putem oferi, le puteți găsi pe

www.pras.ro

PRAS Consulting®
reliable IT solutions

L·O·A·D

Linux Open
Alternative Days

LOAD 10.0 - Thinking to the Future

The 10th Edition