ITCHANNEL

NR. 10, ANUL 5 ● AUGUST 2016 ● www.ITChannel.ro ● IT MAGAZINE FOR TOMORROW

VERITAS - EXCELENȚĂ ÎN MANAGMENTUL INFORMAȚIILOR

Interviu cu Vasile Aniculăesei, Teritory Manager (România, Bulgaria, Grecia și Cipru) - Veritas

>>> pag. 4-5

TREND MICRO și noile vulnerabități ale sistemelor informatice

>>> pag.16-17

ANIS - industria de software și servicii a depășit 3 miliarde de EUR în 2015

>>> pag.8-8

Digital Guardian - noi tendițe pe zona de DLP

>>> pag.6-7

EuroCloud

EuroCloud Forum 2016

5 - 6 October | Bucharest | Romania

Creating new frontiers in European Cloud
5-6 October, Bucharest, Romania

Join the **largest European forum on the future of Cloud**, taking place at Romexpo, in Bucharest on 5-6 October 2016. Held in Romania for the first time, the 7th edition of **EuroCloud Forum** will bring together **900+** representatives of cloud consumers and providers, policy makers, government representatives and many more from across Europe.

Introducing some of our speakers:

Pearse o'Donohue
Head of Unit, Software and Services, Cloud,
European Commission

Dr. Michaela Iorga
Senior Security Technical Lead for Cloud Computing,
National Institute of Standards and Technology
USA

Dr. Bob Jones
HNSciCloud cloud service procurement project leader,
CERN

Linda Strick
Coordinator CloudForEurope,
Fraunhofer Fokus

Dr. Alexander Tettenborn (TBC)
Trusted Cloud Quality Label,
German Federal Ministry of Economics and Technology
BMWi,USA

Danilo Poccia
EMEA Evangelist,
Amazon Web Services

Plus many more! Check the website periodically for updates.

Find out more and register on www.forum.eurocloud.org.

Partners

VEEAM Fabasoft

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

Bogdan ION
Securitate

DREPTUL DE A FI UITAT

Silviu COJOCARU
Redactor-șef ITChannel

Noua reglementare General Data Protection Regulation – GDPR acordă autorităților europene de protecție a confidențialității informațiilor prin impunerea de amenzi care pot ajunge la o valoare de 4% din cifra anuală mondială sau 20 de milioane de Euro pentru încălcările serioase ale directivei. Amenzile pot însemna un risc financiar și de afaceri semnificativ și vor determina acordarea unei importanțe deosebite confidențialității datelor personale.
Reglementarea UE GDPR își propune să aducă protecția de date în era Big Data și Cloud Computing, transformând protecția de date într-un drept fundamental, reglementat uniform și coerent în întreaga Europă. Orice companie care deservește clienți europeni și prelucrează datele personale ale acestora va trebui să se supună acestei legi – chiar și companiile care au sediul și administrează aceste date personale în afara Europei.

Noua reglementare va intra în vigoare din mai 2018, iar companiile vor avea la dispoziție doi ani să se alinieze cerințelor GDPR. Organizațiile care încheie mai devreme acest proces se vor bucura de controlul sporit al datelor, iar managementul mai bun al informației va ajuta la folosirea eficientă a resurselor de stocare, și va evidenția noi perspective valoroase asupra informațiilor stocate.
GDPR introduce noi principii, precum „dreptul de a fi uitat” și obligațiile de notificare. Prin urmare, în anumite circumstanțe, o companie poate fi nevoită să șteargă complet datele personale dacă un utilizator solicită acest lucru. De asemenea, indivizii afectați de o breșă de informații trebuie notificați fără întârzieri nejustificate dacă informațiile lor personale au ajuns în posesia unor entități neautorizate, iar breșa aduce o amenințare serioasă drepturilor și libertăților lor.

Realitatea îngrijorătoare este că majoritatea companiilor nu pot distinge compoziția a jumătate din volumul de date pe care le stochează. Conform Global Databerg Report, 52% din totalul informațiilor stocate și procesate în prezent de către organizații din toată lumea sunt estimate a fi date nestructurate. Această lipsă de vizibilitate le va îngreuna căutarea de informații în datele stocate.

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)

E-ISSN 2285 – 4967

VERITAS – EXCELENȚĂ ÎN MANAGEMENTUL INFORMAȚIILOR

Symantec a anunțat, la începutul anului, finalizarea procesului de vânzare a companiei de management al informației din cadrul grupului, cunoscută sub numele de Veritas, către un grup de investitori din care fac parte: The Carlyle Group, GIC (fondul de investiții suveran al statului Singapore) și alți co-investitori. Valoarea tranzacției a fost de 8 miliarde USD. La aproximativ șase luni de la finalizarea uneia dintre cele mai celebre scindări din industria IT, am vorbit cu Vasile Aniculăesei Teritory Manager – Veritas pentru România, Bulgaria, Grecia și Cipru despre principalele schimbări care s-au produs în cadrul companiei.

Legat de această rupere a companiei Veritas din cadrul companiei Symantec, Vasile Aniculăesei ne-a declarat: *"Acum ceva timp exista o <<mantră>> a firmelor de consultanță care spunea că numai companiile foarte mari pot obține economii de scară și un avantaj competitiv. Astăzi, aceste trenduri tind să se schimbe. Se pare că trebuie să redevii mic, recâștigând pe linie de agilitate, pentru a descoperi noi posibilități de creștere."*

"La aproximativ un an și jumătate de la primul anunț privind separarea Veritas de Symantec, constat plusuri semnificative la viteza de reacție, cea de decizie și în ceea ce privește dinamismul proceselor de afaceri din cadrul companiei. Focusul exclusiv al companiei Veritas pe zona de soluții de managementul informațiilor a permis concentrarea investițiilor și dezvoltarea acestor aplicații într-un ritm accelerat. În ultimul an, s-au lansat versiuni noi pentru majoritatea soluțiilor Veritas, iar roadmapul următoarelor luni reflectă efortul investuțional major făcut de compania noastră."

Noi provocări privind managementul informațiilor

"Volumul de date crește cu o viteză uluitoare, iar informația se răspândește pe servere și în cloud. Creșterea necontrolată a volumului de date este costisitoare pentru mediul de afaceri și poate pune în pericol securitatea acestor date. Astfel, produsele Veritas permit organizațiilor să recunoască valoarea propriilor informații, pentru a-și atinge obiectivele mai rapid și mai eficient. În România, există oportunități majore de dezvoltare în domeniile adresate de Veritas prin portofoliul amplu de soluții pentru managementul și guvernanța informațiilor, menit să sprijine clienții din România să valorifice puterea informațiilor pe platforme locale și în cloud." a pecizat Vasile Aniculăesei.

"Alături de creșterea volumului de date, companiile se confruntă și cu un nivel tot mai ridicat de fragmentare al acestora. Astăzi, datele sunt stocate pe diverse dispozitive și în diverse centre de date, aceste lucruri conducând la dificultatea proceselor de backup și restaurare a datelor." a continuat Vasile Aniculăesei.

32% din datele stocate și procesate de o companie sunt redundante, învechite sau nu au nicio legătură cu activitatea companiei,

în timp ce peste 54% sunt date al căror conținut nu este cunoscut și nu a fost explorat de organizație, conform studiului Databerg Report 2015 realizat de Veritas în rândul a 1.475 de respondenți din 14 țări din Europa Centrală și de Est, Orientul Mijlociu și Africa.

Astfel, doar 14% dintre datele unei companii sunt cu adevărat critice pentru business, arată raportul Veritas, care a analizat modul în care organizaţiile europene din sectorul public şi privat îşi gestionează datele. Dincolo de cantitatea ridicată de date nefolositoare, un factor de risc important este și faptul că angajaţii tratează sistemele IT ale companiei ca pe propria lor infrastructură, ceea ce poate duce la pierderea sau utilizarea necorespunzătoare a datelor critice ale organizației. *"Veritas se află într-o poziție unică pe piață, fiind în măsură să ofere soluții capabile să facă ordine în acest volum imens de date. Data Insight este una dintre soluțiile de referință, capabile să ofere un suport în organizarea informațiilor companiei."* a precizat Vasile Aniculăesei.

Lider de 12 ani în studiile Gartner

Veritas este de 12 ani lider în studiile Gartner Magic Quadrant pentru zona de arhivare și enterprise backup.

"Veritas este singurul furnizor care și-a păstrat statutul de lider în această perioadă în studiile Gartner. Dincolo de studii și poziționarea noastră pe piață, din păcate piața locală este dominată de mentalități privind prețurile aplicațiilor enterprise. Nu există o soluție enterprise care să fie în același timp cea mai bună și cea mai ieftină de pe piață. Să fii lider într-o zona de soluții enterprise presupune investiții imense pe zona de cercercetare – dezvoltare, care vin la pachet cu niște funcționalități unice pe piață. În România, sunt comparate în licitații soluțiile globale lider de piață cu soluții dezvoltate de mici firme locale. Rezultatele acestor investiții în cercetare - dezvoltare, respectiv capabilitățile tehnice superioare ale produselor rezultate, se reflectă în mod necesar în preț." a precizat Vasile Aniculăesei.

Facts & Figures Veritas Software

Veritas Software este una dintre cele mai longevive companii pe zona de infrastructură, fiind înființată în anul 1983 de către doi foști ingineri de la Intel (numele inițial al companiei a fost Tolerant Systems).
Symantec a achiziționat businessul Veritas în anul 2005, valoarea estimată a achiziției fiind la data respectivă de 13,5 miliarde USD. Procesul de separare a companiei Veritas de Symantec a fost finalizat în februarie a.c.

Impactul cloud

"În țările pe care le coordonez, nu am observat reduceri semnificative ale pieței on premises versus cloud. Am constatat că facilitățile produselor pentru cloud, chiar dacă nu sunt folosite pe scară largă în această regiune, sunt apreciate de clienți. Veritas a fost dintotdeauna o companie independentă de alți vendori. Întâi de toate a fost vorba de independența față de hardware, iar acum discutăm de independența față de soluțiile de cloud. Astfel, în produsele noastre au fost integrați conectori de cloud pentru cele mai multe platforme (Google, Amazon, Azure etc.).

De asemenea, suntem una dintre puținele companii care oferă soluții pentru migrarea în cloud. Soluțiile Veritas permit ca la momentul T0 un client să implementeze o soluție de la un furnizor de cloud, iar la momentul T1 să poată migra la alt furnizor. Este oferită astfel o flexibilitate ridicată, evitând situația clienților captivi, pentru situațiile în care nu sunteți mulțumiți de serviciile unui furnizor de cloud sau între timp au crescut semnificativ costurile." a precizat Vasile Aniculăesei.

GDPR și noi reglementări în ceea ce privește securitatea informației

General Data Protection Regulation (GDPR) este un regulament prin care Comisia Europeană intenționează să consolideze și să unifice protecția datelor în cadrul Uniunii Europene (UE). Se adresează, de asemenea, exportului de date cu caracter personal în afara UE. Obiectivele principale ale Comisiei de GDPR sunt de a oferi cetățenilor controlul datelor lor cu caracter personal și pentru a simplifica mediul de reglementare pentru afaceri internaționale, prin unificarea regulamentului în cadrul UE.

"Noua reglementare GDPR urmează să intre în vigoare din anul 2018, ea conducând la schimbări majore privind infrastructura IT a organizațiilor. Conceptul <<Right to be Forgotten>> impus de această reglementare, presupune nu numai ștergerea datelor privind utilizatorii, dar și capacitatea de a demonstra că aceste date au fost efectiv șterse. În contextul GDPR, Veritas se află într-o poziție unică pe piață prin soluțiile pe care le deține în portofoliu." a concluzionat Vasile Aniculăesei.

Silviu Cojocaru

DIGITAL GUARDIAN – NOI TENDINȚE PENTRU ZONA SOLUȚIILOR DLP

Soluțiile de tip DLP (Data Loss Prevention) au căpătat un rol tot mai important pe zona de securitate. Digital Guardian este, potrivit studiului Magic Quadrant realizat de Gartner, unul dintre liderii pieței de specializate de soluții. Am stat de vorbă cu Luke Brown (Vicepreședinte & General Manager, EMEA, India & LATAM – Digital Guardian) și cu Ralph Skoruppa (Channel Manager – Digital Guardian) despre principalele obiective ale companiei.

Software-ul de prevenire a pierderilor de date (Data Loss Prevention) este conceput pentru monitorizarea, detectarea și blocarea transmiterii datelor sensibile. În incidentele de scurgere de date, date sensibile sunt divulgate personalului neautorizat, fie de persoane rău intenționate sau din greșeală sau neatenție. Astfel de date sensibile pot veni sub forma de informații private sau de companie, proprietate intelectuală (IP), informații financiare, datele de card de credit, precum și alte informații, în funcție de afaceri și de industria în care activează firma.

Digital Guardian este unul dintre jucătorii importanți pe piața de securitate. Soluțiile DLP aflate în portofoliul companiei se află în cadranul liderilor, potrivit studiului realizat de Gartner. *"Poziționarea în topul soluțiilor de tip DLP este o consecință a investiției permanente în cercetare și dezvoltare. În prezent, considerăm că avem una dintre cele mai competente echipe pe zona DLP și investim permanent în dezvoltarea echipei. Spre exemplu, ultima investiție de 66 milioane USD a unui fond de investiții în companie a fost dirijată, în cea mai mare parte, pe zona de cercetare-dezvoltare. "* a precizat Luke Brown (foto).

Studiul Gartner Magic Quadrant oferă o imagine completă asupra unei piețe de soluții. Jucătorii pe o anumită piață (e.g. piața de soluții DLP) sunt clasificați în funcție de două criterii principale: viziunea și strategia de dezvoltare a soluțiilor; capacitatea de execuție și de implementare a noilor facilități în cadrul produselor.

DLP și reglementarea pieței

"Acceptarea soluțiilor DLP pe piața românească și cea est-europeană este încă într-o stare incipientă. Rezultatul acestei lipse de acceptare este rezultatul inexistenței reglementărilor pentru diverse verticale profesionale. În SUA și în Europa de Vest, domeniile și problemele de securitate sunt atent reglementate. Spre exemplu, în domeniul financiar-bancar există foarte multe reglementări pentru protecția informațiilor sensibile, multe dintre acestea nefiind încă disponibile pe piața românească. În momentul în care aceste reglementări devin obligatorii pentru piața locală, considerăm că soluțiile DLP vor înregistra o evoluție deosebită. " a declarat Luke Brown.

Ralph Skoruppa a precizat: *"Suntem convinși că piața est-europeană va înregistra o creștere importantă. În acest sens, unul dintre obiectivele noastre importante este dezvoltarea canalului de distribuție. "*

"Piața est-europeană este însă extrem de fragmentată, iar din acest motiv am realizat o strategie de marketing <<two tier>>. Romsym Data joacă un rol important în strategia de dezvoltare în această regiune, fiind distribuitorul nostru în România, Serbia, Bulgaria și Republica Moldova. Romsym Data are un important know-how pe zona de securitate, precum și resurse pe zona de training." a declarat Ralph Skoruppa.

Magic Quadrant

Fondată ca Verdasys în 2002 și rebranduit în 2014, Digital Guardian are sediul în Waltham, Massachusetts. Digital Guardian a achiziționat Cod Green Networks în octombrie 2015.

Soluția Digital Guardian pentru endpointuri se referă la detecția DLP si Endpoint Detection and Response (EDR) fiind disponibilă sub forma unui agent care poate fi instalat pe desktop-uri, laptop-uri și servere care rulează Windows, Linux sau Apple OS X, oferind și suport pentru medii VDI și infrastructură desktop virtuală.
Potrivit Gartner, avantajele soluției sunt:

■Digital Guardian oferă unul dintre cele mai avansați si puternici agenți de tip DLP endpoint integrați la nivel de kernel al sistemului de operarare. În plus față de Windows, sunt suportate Apple OS X și Linux în medii desktop sau de tip server.
■Digital Guardian are capacități puternice pentru a sprijini în cazuri complexe care implică furtul de proprietate intelectuală și protecția secretului prin conținut.
■Clienții raportează timpi de implementare mai rapidă și proiecte de succes atunci când se utilizează atât programele "on premises" Digital Guardian, dar și în situațiile în care soluția este disponibilă ca Managed Security Program. (MSP).
■Strategia Digital Guardian demonstrează o înțelegere puternică a tehnologiei de securitate și a reglementărilor impuse diferitelor domenii pe zona de securitate.

Distribuitor Digital Guardian: www.romsym.ro

Romsym Data – eveniment dedicat noilor reglementări pe zona de securitate

Romsym Data a organizat evenimentul "GDPR, Directiva NIS si viitoarea lege a securitatii cibernetice", eveniment dedicate noilor reglementări pe zona de securitate și soluțiilor capabile să răspundă acestor provocări.

Sistemele informatice actuale pot fi grav afectate de incidente de securitate, cum ar fi defecțiunile de ordin tehnic și virușii. Aceste tipuri de incidente, denumite adesea incidente legate de securitatea rețelelor și a informației (NIS), devin din ce în ce mai frecvente și mai dificil de abordat.

Multe întreprinderi și guverne din întreaga UE se bazează pe infrastructuri și rețele digitale pentru furnizarea serviciilor lor esențiale. Acest lucru înseamnă că atunci când apar incidente legate de NIS, ele pot avea un impact enorm prin compromiterea serviciilor și întreruperea funcționării corespunzătoare a întreprinderilor. În plus, odată cu dezvoltarea pieței interne a UE, numeroase rețele și sisteme de informații funcționează dincolo de frontiere. Producerea unui incident legat de NIS într-o țară poate avea, prin urmare, efecte în alte țări și chiar în întreaga UE. De asemenea, incidentele de securitate subminează încrederea consumatorilor în sistemele de plată online și în rețelele informatice.

Prin introducerea mai multor măsuri consecvente de gestionare a riscurilor și a unei raportări sistematice a incidentelor, propunerea de directivă ar permite sectoarelor care depind de sistemele informatice să fie mai fiabile și mai stabile.
General Data Protection Regulation (GDPR) este un regulament prin care Comisia Europeană intenționează să consolideze și să unifice protecția datelor în cadrul Uniunii Europene (UE). Se adresează, de asemenea, exportului de date cu caracter personal în afara UE. Obiectivele principale ale Comisiei de GDPR sunt de a oferi cetățenilor controlul datelor lor cu caracter personal și pentru a simplifica mediul de reglementare pentru afaceri internaționale, prin unificarea regulamentului în cadrul UE. În cazul în care GDPR intră în vigoare îl va înlocui directiva privind protecția datelor din 1995.

STUDIU ANIS: INDUSTRIA DE SOFTWARE ȘI SERVICII IT A DEPĂȘIT ÎN 2015 VALOAREA DE 3 MILIARDE DE EURO

Conform studiului "Software and IT Services in Romania" lansat de ANIS - Asociația Patronală a Industriei de Software și Servicii, cifra de afaceri a sectorului de software și servicii IT a crescut cu 21% în 2015 comparativ cu 2014, atingând 3,08 miliarde de euro.

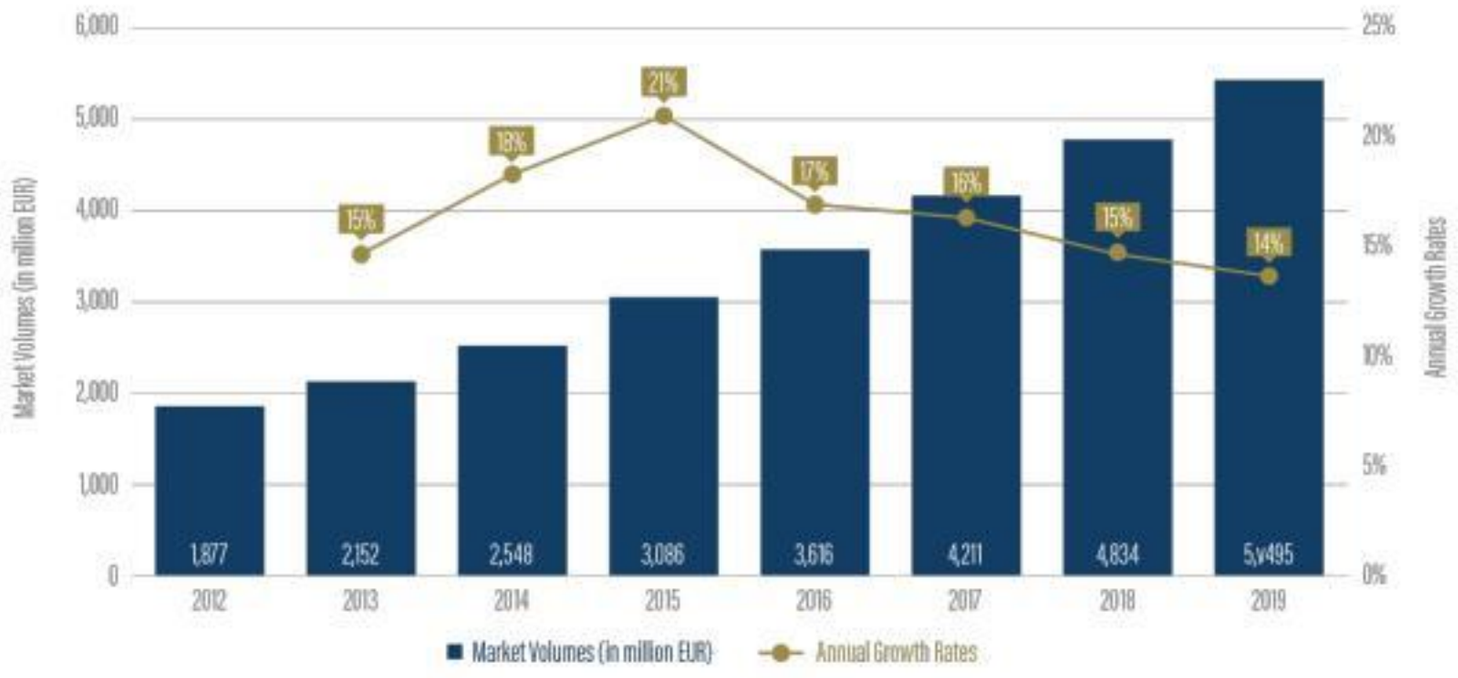
Industria de software depășește astfel previziunile de creștere anunțate în ediția anterioară a Studiului ANIS, estimate la aproximativ 14%. Tendința de creștere este în continuare susținută, prognoza pentru 2016 fiind de peste 17%, ceea ce va ridica cifra de afaceri a industriei la 3,6 miliarde de euro.

Prognoza de creștere medie anuală pentru următorii 5 ani este de 15%, de asemenea în creștere față de estimarea de 11% comunicată în 2015.

Exportul de software și servicii IT a ajuns în 2015 la 2,09 miliarde de euro, cu peste 31% mai mult faţă de 2014, reprezentând 67% din cifra de afaceri a sectorului. Estimările arată că în 2016 valoarea exporturilor va ajunge la 2,5 miliarde de euro, ceea ce reprezintă mai mult decât dublul valorii înregistrate în urmă cu 4 ani.

În ceea ce priveşte piaţa internă, care reprezintă aproximativ 33% din veniturile totale ale sectorului, aceasta a înregistrat o creştere timidă faţă de anul precedent de aproximativ 4%, atingând 991 milioane de euro. Analiza evoluției pieței interne arată ca estimarea de creştere este de aproximativ 4,6% pentru anul în curs, ceea ce reprezintă manifestarea unui consum încă scăzut de tehnologie, mai ales în comparație cu potențialul și nevoile estimate, atât în domeniul public, cât și în cel privat.

Fig. 2 | Romania - Total SITS Industry - Volumes and Growth Rates



Software and IT services in Romania 2016

Având ca motor de creștere cererea mare dinspre Europa de vest și structura de cost încă foarte atractivă, creșterea industriei de software și servicii IT din România este limitată de lipsa disponibilității resurselor pe care clienții le caută, atât ca număr, cât și ca set de abilități.

Se estimează că industria de software și servicii IT va genera mai mult de 3% din PIB-ul României în 3 ani, cu condiția să reușească să treacă de barierele sistemului de educație, prin creșterea numărului de persoane angajate, și să integreze mai mulți angajați străini (în special din Ucraina, Bulgaria, Serbia etc.) care au abilitățile de care industria are nevoie.

Dat fiind că se bazează în primul rând pe capitalul uman și că firmele își pot recompensa salariații cu salarii mult peste media pe economie, industria de software și servicii IT este cu siguranță un vector de creștere pentru reputația, prosperitatea și stabilitatea țării.

Pe termen mediu, este vizibilă tendința de a crește valoarea adăugată a serviciilor IT furnizate din Romania, în timp ce focusul este în continuare pe creșterea numărului de angajați cu set primar de abilități, pentru care diferența de cost față de țările din vest este semnificativă.

Pe termen lung, estimăm că se va consolida poziționarea României ca furnizor pentru servicii cu valoare adăugată mare, centre R&D și proiecte semnificative pentru piața internă care să includă soluții și tehnologii de ultimă generație.

PAC, de-a lungul celor mai bine de 17 ani în care a activat pe piața serviciilor de cercetare și consultanță strategică, a remarcat o evoluție interesantă a celor 2 segmente care compun industria românească de software și servicii IT: piața locală și respectiv exportul de servicii IT, dezvoltarea de produse software proprietare generând o pondere relativ mică în cifra de afaceri totală a sectorului.

Din 2008, aceste 2 segmente au crescut cu viteze semnificativ diferite și ne așteptam ca, în principal pe fondul lipsei de resurse umane, ratele de creștere să continue într-un ritm similar celui de

până acum, astfel contribuind la accentuarea diferenței volum.
Estimăm ca exportul de software și servicii IT va ajunge în 2016 la 2,5 miliarde de euro, care este mai mult decât dublul valorii înregistrate în urmă cu 4 ani, în timp ce în aceeași perioadă piața internă a crescut cu mai puțin de 200 de milioane de euro.
Piata românească de software si servicii IT a fost afectată de mai mulți factori interni și externi, care i-au influențat creșterea și respectiv șansele furnizorilor din acest sector de a crește sau chiar de a continua să existe.
Cu o maturitate a mediului de business care o plasează în urma Poloniei, Cehiei, Ungariei sau Slovaciei, România este singura țară din regiune în care un număr mic de furnizori au acoperit aproape întreaga piață de soluții IT complexe pentru sectorul public și companiile publice, în special în energie, dar și în transporturi, relația cu puterea politică jucând un rol important în această situație.
In ultimii 3-5 ani, mai multe dintre companiile locale mari integratoare de sisteme IT au fost subiectul unor investigații legate de corupție și/ sau evaziune fiscală, ceea ce a făcut ca unele dintre acestea să intre în insolvență, iar altele să își restructureze semnificativ afacerile.
Piața locală private este concentrată în jurul multinaționalelor, în cazul cărora discutăm de contracte cu valori de până la câteva milioane de euro, deși alocările bugetare locale sunt nesigure chiar și pentru aceștia. Totuși, există semne clare de maturizare a pieței IT locale, a managerilor IT / Chief Information Officer și a managerilor companiilor. Tipurile de soluții adoptate de companii arată un interes crescut pentru tehnologii orientate către business, care presupun costuri scăzute și generează recuperarea rapidă a investiției.
Climatul general în sectorul privat rămâne caracterizat de decizii luate încet și cu grijă, bugetele sunt cheltuite doar pentru îndeplinirea obiectivelor clare și direcționate, pe termen scurt. Cele mai multe companii sunt reticente în a lansa proiecte livrate în întregime de furnizori, ceea ace face ca modelul "time & material" să fie încă foarte popular.
Centrele offshore s-au dezvoltat semnificativ și continua să crească foarte repede, fiind susținute de facilități fiscale, o populație semnificativă de resurse cu înaltă calificare și tendința în creștere dinspre pieţele mature (in special Europa de vest și SUA) de a scădea costurile pentru dezvoltarea software și serviciile IT.

Totuși, această creștere nu s-a concentrat până acum pe dezvoltarea de produse software cu valoare adăugată mare sau servicii IT critice, ci mai ales pentru serviciile de suport cu valoare adăugată mică, codare și management de aplicații, unde diferența de costuri este cea mai mare.
In ce privește acționariatul companiilor de software și servicii IT, vom observa că investitorii strategii (corporațiile IT) și antreprenorii locali au fost cei mai activi în ultimii 10 ani. Fondurile de investiții și investitorii individuali sunt din ce în ce mai vizibili pe piață, analizând diferite oportunități de implicare în companiile IT locale cu potențial.

In contextul actual în care companiile multinaționale mari domină clar sectorul de software și servicii IT, este evident că șansa antreprenorilor locali este aproape exclusiv dezvoltarea de servicii cu valoare adăugată mare și/ sau produse software care țintesc piața globală.
Produsele software de nișă adresate doar pieței locale nu pot genera volume de business semnificative pentru a susține creșterea, iar soluțiile IT generice pentru pieţele globale nu pot fi competitive prin comparație cu alți furnizori deja prezenți pe pieţele țintă.

Despre studiu
Studiul „Software and IT Services in Romania 2016" este un proiect ANIS realizat de PAC – Pierre Audoin Consultants și se află la a treia ediție. Raportul este disponibil pentru comandă pe pagina dedicată – http://itstudy.anis.ro/

Fig. 4 | Romania - Total SITS Industry - Market destination - Volumes and Growth Rates

TRANSFOND

Despre TRASFOND

TRANSFOND este operatorul tehnic al **Sistemului Electronic de Plăţi din România**, precum și furnizor de servicii de facturare şi arhivare electronică. Compania şi-a demarat activitatea în centrul comunităţii financiare din România în scopul realizării și administrării Sistemului Electronic de Plăți Interbancare.

Prin infrastructura pe care a dezvoltat-o, TRANSFOND consolidează o nouă arie de dezvoltare - servicile e-business, menite să înlesnească activitatea companiilor din zona financiară. Dezvoltarea unor servicii cu valoare adăugată, care să aducă eficientizarea activității pentru companii, reprezintă una dintre principalele preocupări ale TRANSFOND.

TRANSFOND are experienţă în coordonarea de proiecte de mari dimensiuni, cu multe instituţii implicate, ale căror interese sunt diferite în funcţie de tipurile de servicii prestate, cu viteze şi metodologii de lucru diferite, cu infrastructuri care variază foarte mult. Rezultatele obţinute în urma acestor proiecte au fost pe deplin apreciate de beneficiarii lor - băncile comerciale românești.

Situatia initiala

"Proiectul inițial a avut ca obiect protejarea informațiilor companiei, această nevoie de protecție fiind derivată din mai multe standarde de securitate și din riscurile specifice acestui domeniu de activitate. Sectorul financiar-bancar este caracterizat printr-un nivel ridicat al riscului reputațional." a precizat Marian Simion, CIO – TRANSFOND.

"Proiectul a început acum cinci ani prin achiziționarea Symantec DLP. Într-o primă etapă, ne-am propus ca partea de clasificare să fie realizată cu mijloace interne, fără a utiliza o soluție specializată. Ulterior am observat că acest proces nu este foarte simplu, mai ales din perspectiva utilizatorilor finali. Disciplina, regulile îmbunătățite de securitate a documentelor, obișnuința de a le marca, reprezintă

"Implementarea soluției Titus a permis clasificarea facilă a tuturor documentelor existente la nivelul organizației. Acest lucru a avut ca finalitate un control mai bun al documentelor pe tot ciclul de viață al acestora."

Marian Simion, CIO - TRANSFOND.

rutine noi de securitate a informației pentru utilizatorii interni. Decizia ulterioară de a implementa suita de clasificare de la Titus ne-a sprijinit în acest proces de acomodare cu noile practici în materie." a completat Marian Simion.

Solutia

"Content-Aware" Data Loss Prevention (DLP) este o tehnologie de securitate cu un grad avansat de inteligență, bazată pe descoperirea și analiza de conținut și context a expunerii datelor confidențiale. DLP analizează, monitorizează și protejează în timp real datele confidențiale ale unei organizații, fără a constrânge utilizatorii, prin limitări tehnice, în folosirea corectă a datelor în conformitate cu procedurile definite.

Prevenirea scurgerilor de date confidențiale rezultă dintr-o îmbinare a tehnologiei cu procesul de educare a angajaților și cu rafinarea politicilor de securitate ale companiilor.

Reglementările guvernamentale și cele impuse la nivel de verticale profesionale joacă un rol tot mai important, DLP devenind o componentă obligatorie a celor mai importante standarde și reglementări actuale (PCI, Basel 2, HIPAA, Sarbanes-Oxley, etc.). Tehnologia DLP de la Symantec oferă un suport complet pentru implementarea acestor reglementări, fiind plasată de Gartner în cadranul liderilor de piață.

Soluția DLP de la Symantec, s-a bucurat de o adopție rapidă în piețele avansate: o treime din companiile FORTUNE100, 9 dintre primele 10 bănci comerciale și de investiții la nivel global, 6 din primele 10 companii de asigurări, 6 dintre cele mai mari companii energetice, 8 dintre cele mai importante firme de producție, precum și mari companii din sectoarele Telecom, Healthcare, Retail și Guvernamental din SUA.

Soluția TITUS de securitate automatizează procesul de clasificare și marcare a documentelor în cadrul organizației. Soluția este perfect integrată cu suita Microsoft Office, serverul Exchange și aplicația Outlook, precum și cu aplicația Acrobat dedicată creării și gestionării documentelor în format PDF.

"Un avantaj important al soluțiilor Titus este integrarea cu suita de aplicații Microsoft și procesul foarte simplu prin care utilizatorii pot marca și clasifica documentele. Practic, aplicațiile Titus sunt integrate nativ cu soluțiile Microsoft, utilizatorii realizând aceste operațiuni direct din interfețele programelor Word, Excel sau Outlook." a precizat Marian Simion.

"În procesul de alegere a soluțiilor Symantec și Titus, am pornit de la o serie de referințe importante existente pe piața locală și de la studiile realizate de marile companii de analiză de piață. Studiul Magic Quadrant, realizat de Gartner, a jucat un rol important în această alegere. În procesul de selecție, ne-am focalizat pe soluțiile existente în cadranul liderilor. De asemenea, un criteriu foarte important în selecția soluțiilor a fost existența suportului în România pentru acestea." a precizat Marian Simion.

"Suplimentar, cele două soluții ne-au ajutat la procesul de recertificare ISO 27001. Prin integrarea soluțiilor Symantec DLP și Titus Classification, am avut deja implementate anumite controale și cerințe specifice acestui standard de securitate" a declarat Marian Simion.

Legat de implementare, Marian Simion a declarat: *"Procesul de implementare și integrare a decurs foarte bine pentru cele două soluții. Timpul de implementare a fost foarte scurt (aproximativ 3-4 luni pentru fiecare soluție), iar relația cu Infodava s-a desfășurat foarte bine și în termenele stabilite."*

Beneficii

"Implementarea soluției Titus a permis clasificarea facilă a tuturor documentelor existente la nivelul organizației. Acest lucru a avut ca finalitate un control mai bun al documentelor pe tot ciclul de viață al acestora.

De asemenea, implementarea soluției de clasificare a condus la o responsabilizare a utilizatorilor, soluția fiind acceptată și chiar bine primită de aceștia. Ținând cont de aceste beneficii, putem considera că eficiența soluției DLP a crescut semnificativ în ceea ce privește procesul de monitorizare a documentelor în cadrul organizației și în relație cu terțe părți." a concluzionat Marian Simion, CIO - TRANSFOND.

INFODAVA

REGUS WTC BUCURESTI, PIATA MONTREAL 10, INTR. F,

SECTOR 1, BUCHAREST, ROMANIA

PHONE/FAX: +40 31 107 34 25

WWW.INFODAVA.COM

FACEBOOK.COM/INFODAVA

EMAIL: OFFICE@INFODAVA.COM

10 Years

INFODAVA

VERITAS PREGĂTEȘTE ORGANIZAȚIILE PENTRU CEA MAI MARE SCHIMBARE A LEGILOR DE PROTECȚIE A DATELOR DIN ULTIMII 20 DE ANI

Veritas Technologies, lider global în domeniul managementului informației, anunță soluții și servicii care vin în sprijininul organizațiilor care vor implementa noua Reglementare europeană în privința protecției de date cu caracter general (General Data Protection Regulation – GDPR), recent promulgată de către Parlamentul Uniunii Europene. Veritas Enterprise Vault™ 12, Data Insight 5.1, Information Map și serviciile asociate oferă companiilor vizibilitatea necesară asupra informațiilor nestructurate pentru a se putea conforma mai bine atât noilor reglementări GDPR cât și celor deja existente..

Noua reglementare acordă autorităților europene de protecție a confidențialității informațiilor prerogative pentru impunerea de amenzi care pot ajunge la o valoare de 4% din cifra anuală mondială sau 20 de milioane de Euro pentru încălcările serioase ale directivei. Amenzile pot însemna un risc financiar și de afaceri semnificativ și vor determina acordarea unei importanțe deosebite confidențialității datelor personale.

Reglementarea UE GDPR își propune să aducă protecția de date în era Big Data și Cloud Computing, transformând protecția de date într-un drept fundamental, reglementat uniform și coerent în întreaga Europă. Orice companie care deservește clienți europeni și prelucrează datele personale ale acestora va trebui să se supună acestei legi – chiar și companiile care au sediul și administrează aceste date personale în afara Europei.

Noua reglementare va intra în vigoare din mai 2018, iar companiile vor avea la dispoziție doi ani să se alinieze cerințelor GDPR. Organizațiile care încheie mai devreme acest proces se vor bucura de controlul sporit al datelor, iar managementul mai bun al informației va ajuta la folosirea eficientă a resurselor de stocare, și va evidenția noi perspective valoroase asupra informațiilor stocate.

Cultura acumulării de date creează volume mari de date nestructurate

GDPR introduce noi principii, precum „dreptul de a fi uitat” și obligațiile de notificare. Prin urmare, în anumite circumstanțe, o companie poate fi nevoită să șteargă complet datele personale dacă un utilizator solicită acest lucru. De asemenea, indivizii afectați de o breșă de informații trebuie notificați fără întârzieri nejustificate dacă informațiile lor personale au ajuns în posesia unor entități neautorizate, iar breșa aduce o amenințare serioasă drepturilor și libertăților lor.

Realitatea îngrijorătoare este că majoritatea companiilor nu pot distinge compoziția a jumătate din volumul de date pe care le stochează. Conform Global Databerg Report, 52% din totalul informațiilor stocate și procesate în prezent de către organizații din toată lumea sunt estimate a fi date nestructurate. Această lipsă de vizibilitate le va îngreuna căutarea de informații în datele stocate.

Veritas face „lumină” în volumele de date stocate

Pentru a-și micșora riscurile, companiile au nevoie să înțeleagă datele stocate, inclusiv porțiunile semnificative de informații nestructurate, stocate fragmentat de-a lungul întregii infrastructuri locale și de cloud. Veritas oferă soluții și servicii pentru a face „lumină” în informații nestructurare.

- Information Map o aplicație nativă de cloud crește vizibilitatea datelor nestructurate. Information Map adună meta-date din NetBackup, și le pune la dispoziție printr-un tool vizual de navigare, care ajută utilizatorii să identifice zone-

le de risc, de valoare și de pierderi din depozitele lor primare de conținut. NetBackup oferă servicii de back-up și recovery pentru întreaga infrastructură IT, indiferent dacă platforma este una virtuală, fizică sau în cloud.

• Data Insight 5.1 sprijină aplicarea și monitorizarea politicilor de administrare a datelor. Companiile au nevoie să înțeleagă cine trebuie să fie autorizat și cine accesează datele personale din sistemul de fișiere corporativ. Acest lucru este dificil, având în vedere mediile de stocare foarte fragmentate, compuse din servere de fișiere, servicii în cloud, diversele dispozitive, back-up-uri și arhive. Data Insight 5.1 de la Veritas rulează analize de date și facilitează managementul retenției, obține conformitatea accesării, și sprijină o mai bună înțelegere a faptului că utilizatorul poate reprezenta un factor de risc pentru informații sensibile.

• Enterprise Vault 12 oferă un cadru centralizat pentru clasificarea automată a informațiilor. Pentru GDPR va fi esențial să se știe unde se stochează datele personale, mai ales în cazul unor formate nestructurate precum documentele excel, prezentările și tabelele. Acest aspect este esențial, atât pentru protecția datelor cât și pentru a răspunde cererilor de corectare și ștergere a datelor personale. Software-ul de arhivare clasifică automat conținutul înglobat, inclusiv e-mail-uri, fișiere, SharePoint, mesagerie instant și social media. În calitatea sa de cel mai important vânzător de programe de arhivare a informației la nivel enterprise, Veritas le oferă clienților care dispun deja de petabiți de informații arhivate capacitatea de a reclasifica aceste informații, într-un mod care să le permită să-și ajusteze politicile de retenție pe termen lung a informației la noile reglementări, precum GDPR.

Pentru mai multe informații, vă rugăm accesați https://veritas.com/product/information-governance/general-data-protection-regulation.html

Enterprise Vault 12

Enterprise Vault oferă companiilor vizibilitate completă asupra informațiilor de business, reduce costurile de backup şi stocare păstrând în acelaşi timp informaţiile importante, transformă procesul de identificare și clasificare a datelor într-o operaţiune restrânsă, repetabilă şi sigură.

În ansamblu, Veritas Enterprise Vault este o platformă de arhivare menită să întrunească cerințele tot mai ample din mediul de business privind gestionarea volumelor de date ale unor departamente cum ar fi business, juridic şi informatic, sprijinind organizaţiile să descopere şi să gestioneze mai bine informaţiile nestructurate, precum şi să stocheze informaţii în mod inteligent.

Alte noi funcţii ale Enterprise Vault 12 includ:

• Intelligent Review – simplifică supravegherea conţinutului arhivat, prin prioritizarea articolelor relevante pentru revizuire şi eliminarea articolelor irelevante, folosind un motor aflat în permanentă optimizare.

• Gated Deletion – îmbunătăţeşte conformitatea cu standardele privind managementul informațiilor, garantând ştergerea datelor arhivate numai dacă acestea îndeplinesc politicile de retenţie curente. Organizaţiile pot executa acum o verificare a politicilor, înainte de expirare sau de ştergerea de către utilizator.

• Image OCR (recunoaşterea optică a caracterelor) – permite căutarea şi descoperirea de imagini arhivate prin extragerea textului încorporat din imagini, pentru indexare şi clasificare.

• Transfer cu costuri zero de la licenţa Data Classification Services la licenţa Enterprise Vault Retention, care include Clasificare, Reclasificare şi Gated Deletion.

Marius Turlea este Tehnology Solutions Manager la Veritas

IoT - ÎNTRE BENEFICII ȘI PROVOCĂRI

Bogdan Ion

Network & Security Engineer

Veracomp Europe

Ştim, noi, oare la ce riscuri ne supunem atunci când îmbrăţişăm IoT-ul? Suntem, oare, conştienţi de pericolele ce pot apărea dacă un răuvoitor (hacker, etc) ne sparge reţeaua şi se conectează la echipamentele noastre? Adică, e evident un mare avantaj să ai o cameră de supraveghere în casă la care te poţi conecta când eşti la birou să vezi ce face bona cu copilul tău minor, dacă a păpat ce trebuie, dacă a dormit, şi dacă s-a purtat frumos cu el. Dar acelaşi lucru îl poate face şi altcineva străin. Mai mult, acel cineva te poate supraveghea şi pe tine în intimitatea casei tale. Asta nu mai sună bine, aşa-i?

Un alt articol pe această temă poate fi citit aici - http://veracomp.ro/blog/securitate/3168-iot-e-nu-asa.html

În continuarea exemplelor IoT pentru utilizatorii individuali, care sunt principalele provocări IoT pe zona de business?

Am tot vorbit de pericolele pe care IoT-ul le aduce, fără să aducem prea mult în discuţie avantajele. Totuşi, este evident că IoT-ul, folosit cum trebuie, ne uşurează viaţa. Cum? Păi să luăm exemplul IoT-ului casnic. Un TV conectat la Internet ne oferă mult mai multe posibilităţi de conectare la servicii video diverse, de la ştiri până la filme şi emisiuni de divertisment. Putem conecta aparatul de aer condiţionat la Internet pentru a seta temperatura ambientală din casă atunci când nu suntem acasă. Frigiderul conectat la Internet şi dotat cu o cameră video ne oferă posibilitatea să verificăm ce avem de mâncare în frigider atunci când plecăm de la birou şi dorim să ne oprim la magazinul de la colţ. Exemple sunt multe, iar avantajele sunt evidente. Sună bine, dar care sunt challange-urile? Lăsând la o parte securitatea, de care am vorbit şi vom mai vorbi, trebuie luat în calcul costul IoT-ului. Ce vreau să spun cu asta? E simplu: un TV cu posibilităţi de conectare la Internet (smart TV) e mai scump decât un TV tradiţional (LCD, LED, sau defuncta – din păcate - plasmă) fără această conectivitate. Aparatul de aer condiţionat are nevoie de un modul special wireless ca să poată fi conectat la Internet = cost adiţional. E evident că un fridiger cu camera video şi conectare la Internet costă mai mult decât un frigider tradiţional. În general, ce conţine SMART în denumire e mai scump (smartphone, smart TV, etc). De asemenea, trebuie luat în calcul faptul că mai multe device-uri conectate la Internet necesită o putere de conectare mai mare, adică un router mai puternic (deci mai scump), o conexiune de Internet mai bună (şi mai scumpă, evident), consum de curent mai mare, etc – toate acestea se traduc în costuri mai mari pentru end-user. De asemenea, pentru providerii de echipamente SMART provocarea e scoaterea pe piaţa de echipamente mai bune, care să facă faţă concurenţei, la un preţ atractiv. Nu în ultimul rând, când vorbim de SMART nu putem vorbi de hardware fără software – asta e ceea ce le face SMART, până la urmă. Prin urmare, dezvoltarea de aplicaţii pentru controlul acestor device-uri şi menţinerea up-to-date a softurilor echipamentelor trebuie să fie continuă.

Cum putem reduce riscurile la care ne expunem la o infrastructură bazată pe IoT?

Am spus în răspunsul de la întrebarea anterioară faptul că IoT-ul ne uşurează viaţa, atunci când e folosit cum trebuie. La ce m-am referit când am spus asta?
În primul rând trebuie să identificăm acele device-uri cu IoT care ne fac viaţa mai uşoară. Nu trebuie să utilăm toată casa cu device-uri SMART, dacă nu le folosim sau nu aduc plus valoare în viaţa noastră, doar că „aşa e moda". În acest caz vorbim de bani aruncaţi pe fereastră şi breşe de securitate mai multe şi mai mari. Din punctul meu de vedere, trebuie să stăm să ne gândim dacă, într-adevăr avem nevoie de acele funcţionalităţi SMART.
Trăim în era vitezei - dacă nu avem timp să ne uităm în frigider să vedem ce e acolo, cu siguranţă nu avem timp să gătim. Prin urmare un frigider SMART devine doar un gadget inutil şi foarte scump. Şi exemplele pot continua.
În al doilea rând, având în vedere că toate aceste device-uri se conectează la Internet, trebuie să securizăm această conexiune. Ca şi prim pas pentru a face acest lucru e să construim o reţea (cu fir sau wireless) cât mai bună şi protejată, cel puţin de o parolă cât mai dificilă (lungă, cu litere mari, mici, cifre, caractere speciale, etc). Apoi putem alege un router wireless cu capabilităţi de criptare cel puţin WPA2. Încă e greu de spart o astfel de parolă, deşi nu imposibil, cum a arătat ultimul timp.
Toate acestea pot fi făcute cu costuri minime. Astfel de soluţii wireless

există în piaţă la preţuri decente şi accesibile oricui. Trebuie doar să ne dăm interesul pentru a ne proteja.

Ce soluții este indicat să folosim pentru a reduce aceste riscuri?

Am menţionat anterior câteva soluţii pentru a ne securiza reţeaua şi a scădea riscurile unei infrastructuri IoT. Totuşi, cele de mai sus aduc un prim pas de securizare, minim, elementar. Pentru a trece la pasul următor, avem nevoie de soluţii dedicate de securitate. Mă refer la acele soluţii care sunt capabile să „ascundă" reţeaua wireless folosită de infrastructură, astfel încât să nu fie vizibilă din exterior. Mă refer la acele soluţii care sunt capabile să filtreze traficul care intră şi iese din reţea la nivel de tip de trafic, server sau client oriented, la nivel de semnături, la nivel de behavior, la nivel de identificare a încercărilor de conectare la reţele botnet C&C, etc. Am vorbit până acum numai de exemplul casnic. Însă, aceleaşi principii sunt valabile şi în mediul business. De exemplu, au apărut imprimante profesionale cu sistem de operare Android. Asta înseamnă că ele sunt vulnerabile la tot ce e vulnerabil în acest sistem de operare. And by all means, Android este cel mai sensibil sistem de operare mobil la atacuri. Imprimantă poate deveni, astfel, un „cuib" perfect pentru diverse programe de tip malware. Ne putem trezi că din reţeaua noastră se lansează atacuri DDoS sau se extrag date fără să ştim acest lucru pentru mult timp. Trebuie să asigurăm securitatea reţelei până la layer 7, să controlăm tot ce intră şi iese în/din reţeaua noastră la nivel de trafic legitim/ilegitim, la nivel de aplicaţie, la nivel de site-uri accesate de utilizatori, conţinut accesat, etc. În acest sens, Fortinet – lider în zona Network Security şi UTM (Unified Threat Management) – vine cu soluţia unificată Fortigate ce oferă protecţie de tip NextGen Firewall, Intrusion Prevention System, Gateway Antivirus, Application Control, Web Filtering. De asemenea, trebuie să identificăm şi să protejăm device-urile care se conectează la reţeaua noastră, atât end-pointurile (laptopuri, PC-uri, telefoane), cât şi serverele, fie că sunt fizice, fie că sunt în cloud, fie că e o reţea de servere hibridă. Este necesar să avem vizibilitate asupra întregului trafic atât la perimetrul reţelei, cât şi în interiorul ei, iar TrendMicro - lider în zona server security, cloud security şi small business content security - vine în întâmpinarea acestei necesităţi cu soluţia Deep Discovery de analiză a traficului, care ne protejează şi de acele atacuri ce vin prin trafic est-vest, aşa zis lateral movement. Totodată, TrendMicro oferă soluţii de ultimă generaţie pentru atacuri de tipul ransomware, cryptolocker, atacuri web sau exploit-uri asupra vulnerabilităţilor software – toate aceste pot fi asociate cu pericolele la care IoT-ul ne expune. Aceşti vendori fac parte din portofoliul Veracomp şi cu ajutorul lor putem crea o reţea cu adevărat sigură. Fiind protejaţi cu astfel de soluţii ne putem bucura, într-adevăr, de avantajele evidente ale IoT-ului.
Nu în ultimul rând, o bună instruire a personalului în ceea ce priveşte securitatea IT precum şi menţinerea sistemelor de operare la zi sunt lucruri absolut necesare.

Alte articole dedicate IoT și zonei de securitate sunt disponibile pe blogul Veracomp:

http://veracomp.ro/blog/

TREND MICRO ȘI NOILE VULNERABILITĂȚI ALE SISTEMELOR INFORMATICE

Trend Micro s-a impus ca unul dintre liderii globali pe zona de soluții de securitate, compania acoperind toate problemele și vulnerabilitățile în ceea ce privește securitatea informatică. Legat de "peisajul" securității IT, unul dintre cele mai dinamice domenii IT&C, Paul Ursu, Trend Micro Business Development Manager la Veracomp, ne-a oferit mai multe informații.

Trend Micro este, la nivel global, unul dintre cei mai importanți producători de soluții de securitate; producătorul a raportat pentru 2015 vânzări totale nete de 1,02 miliarde USD, un profit operațional de 255 milioane USD și un profit net de 176 milioane USD. La începutul acestui an, Veracomp a semnat parteneriatul și a devenit unicul distribuitor Trend Micro pe piața locală.

L-am întrebat pe Paul Ursu care au fost principalele motive pentru care a fost realizat acest parteneriat: *"Trend Micro dispune de un portofoliu complet de soluții de securitate, acestea acoperind toate nevoile unei organizații. Astfel, sunt disponibile soluții pentru utilizatorii individuali (accesibile pe diverse platforme MAC OS, Windows, sisteme de operare pentru dispozitivele mobile etc.), companii mici de până la 100 de utilizatori, precum și pentru zona enterprise. Un alt lucru important, care a contat în realizarea acestui parteneriat, este faptul că Trend Micro este un brand de tip A. În acest sens, atât Gartner, NSS Labs, cât și alte organizații independente atestă că Trend Micro este lider de piață pentru diverse soluții din portofoliu."*

"În comparație cu competitorii, Trend Micro s-a impus prin numărul mare de facilitățile incluse în soluțiile sale. Într-un, <<battlecard>> care compară Trend Micro cu Microsoft ForeFront și celelalte soluții de securitate lider de piață (McAfee și Symantec), soluția noastră este singura care oferă toate facilitățile pe zona de securitate. Trend Micro este singurul furnizor care are integrate funcții avansate pentru atacurile targetate și sandbox, cu mașini virtuale personalizabile. " a declarat Paul Ursu.

Fizionomia unui atac informatic în contextul actual

Observăm o schimbare radicală a modului în care sunt realizate atacurile asupra sistemelor informatice. În trecut, primau atacurile de volum, printre care se numărau și atacurile de tip phishing, atacuri în care erau vizate un număr mare de ținte (sute mii sau milioane de e-mail-uri).

Astăzi, discutăm mai cu seamă de atacuri targetate. *" Studiile Trend Micro arată că aproximativ 75% dintre atacuri sunt de tip targetat. Ce presupune un astfel de atac? În primul rând, o etapa de social engineering în care prin intermediul unor rețele sociale (Linkedin mai cu seamă pentru zona de business) sunt aflate informații despre persoanele cheie din companie (CEO, CFO etc.). După ce sunt aflate aceste date, se realizează atacul efectiv care poate lua diverse forme (spre exemplu, poate fi un mail personalizat către CFO care să includă un link către site-ul de unde se realizează efectiv atacul). De multe ori, site-ul de unde a fost realizat atacul targetat este disponibil mai puțin de o oră, lucru care îl face imposibil de identificat prin mijloace de tip <<web reputation>>."* a declarat Paul Ursu.

Existența pe scară largă a acestor atacuri inteligente și targetate a condus la apariția altor provocări pentru companii: "*Analizele Trend Micro arată că, în medie, de la momentul realizării unui atac la momentul identificării acestuia trec aproximativ două luni. În această perioadă, compania este foarte expusă, putând fi compromise date extrem de importante pentru activitatea acesteia."* a completat Paul Ursu.

Securitate pentru IMM-uri

Companiile mici și medii nu dispun în cele mai multe situații de personal IT specializat pe zona de securitate. În acest context, soluțiile dedicate acestui tip de companii trebuie să fie extrem de accesibile și să dispună de interfețe prietenoase. "Trend Micro Worry Free este o soluție <<out of the box>> foarte simplu de implementat, fiind dedicată companiilor cu până la 100 de utilizatori. Ce aduce nou Trend Micro în această zonă este combinarea, într-o singură soluție, atât a facilităților "on pre-

mises", cât și a celor din cloud. În acest sens, Worry Free protejează serverele, stațiile de lucru și dispozitivele mobile, dar poate fi integrat cu soluțiile de comunicare și colaborare din cloud, fiind oferit suportul nativ pentru Microsoft Office 365 și Google Apps." a declarat Paul Ursu.

Funcționalități avansate pe zona enterprise

Soluțiile Trend Micro dispun de o serie de funcționalități avansate. *"Trend Micro dispune de cel mai avansat Sandbox pentru testarea posibilelor vunerabilități. Sandboxul este bazat pe mașini virtuale (sunt suportate până la 60 de mașini virtuale personalizabile - Trend Micro Deep Discovery Analyzer), în care sunt testate amenințările pe o platformă identică cu cea atacată. Pentru atacurile de tip <<zero day>> (n.r. problemele de securitate care nu au fost încă identificate de producătorul aplicațiilor și pentru care nu există patchuri), Trend Micro a introdus "Digital Vaccine", solutie care protejează împotriva vulnerabilităților pe perioadă ândelungată (spre exemplu, în cazul vulnerabilitatii HeartBleed, vaccinul digital a protejat sistemele timp de 43 de ile, până când grupul OpenSSL a lansat patch-ul împotriva acestui atac. "* a precizat Paul Ursu.

Trend Micro în 24 de ore

- **Sunt analizați 15 TB în 24 de ore**
- **Sunt analizate 1,5 miliarde de posibile amenințări zilnic**
- **Sunt identificate 180.000 de noi amenințări zilnic**
- **Sunt blocate aproximativ 250 de milioane de atacuri**

"Un alt lucru important este că soluțiile Trend Micro nu analizează numai traficul inbound și outbound, ci întreg traficul din cadrul organizației. Pot fi identificate astfel situațiile în care un calculator este compromis în urma deschiderii unor aplicații de pe stick, iar mail-urile trimise către colegi de la acel calculator sunt identificate ca posibile amenințări. Amenințările interne și atacurile începute din interiorul organizației sunt tot mai frecvente acestea afectând tot mai multe companii și producând pagube semnificative. " a continuat Paul Ursu.

Multiple fațete ale securității

Suntem obișnuiți să discutăm despre securitatea ultimelor generații de servere sau alte dispozitive, dar în realitate lucrurile nu stau în tocmai așa. *"În Siberia / Rusia, a fost realizat in 2009 un atac targetat asupra turbinelor unei hidrocentrale (centrala hidroelectrica Sayano-Shushenskaya), din suprasolicitarea acestora ducand la pagube umane si materiale (bilantul tragic a ajuns la 75 de morti, pierdere financiara estimata la 523 milioane USD, pierdere de putere generabila de 6 GW.)*

În zona soluțiilor industriale, Trend Micro este unul dintre puținii producători care oferă soluții de securitate. Dispunem de soluții pentru POS-uri și ATM-uri (Trend Micro Safe Lock), precum și de soluții de securitate pentru servere industriale și mașini CNC care se poate folosi cu versiuni ale sistemelor de operare care pornesc de la Microsoft Windows 2000 SP4, 32biti sau Microsoft Windows Embedded . De asemenea, suntem printre puținii furnizori care au solutii certificate pentru serverele SAP (Trend Micro Deep Security for SAP Systems), sau, Lotus Domino (ScanMail for Lotus Domino, in toate variantele)" a precizat Paul Ursu.

Silviu Cojocaru

RANSOMWARE ȘI NOI PROVOCĂRI PE ZONA DE SECURITATE

Cu prilejul evenimentului anual Veracomp "Zona 9", eveniment tradițional dedicat partenerilor, am stat de vorbă cu Attila Gömbös (Sales Engineer - Trend Micro) despre noile provocări pe zona de securitate. Atacurile de tip "Ransomware" sunt tot mai frecvent întâlnite, iar Trend Micro are o istorie destul de lungă în combaterea acestor atacuri. De asemenea, am vorbit cu Attila Gömbös despre parteneriatul cu Veracomp (parteneriat inițiat în această primăvară) și dezvoltarea canalului de distribuție local.

"Tot mai mulți clienți din mediul privat sau de business sunt victimele unor atacuri de tip ransomware. Ironic este că o parte dintre aceste victime, până nu au nevoie de datele salvate în fișierele comnpromise, nici măcar nu știu că au fost victima unor astfel de atacuri. " a precizat Attila Gömbös.

Ransomware este un tip de malware care împiedică sau limitează accesul utilizatorilor la sistemul lor, fie prin blocarea ecranului sistemului sau prin blocarea fișierelor utilizatorilor, până în momentul în care este plătit un preț de răscumpărare. Atacurile moderne de tip ransomware presupun criptarea anumitor tipuri de fișiere de pe sistemele infectate, iar utilizatorii sunt forțați să plătească răscumpărarea prin intermediul unor metode de plată on-line pentru a obține o cheie de decriptare.

"Trend Micro are o serie întreagă de soluții care elimină riscul unor atacuri de tip Ransmoware. Aceste soluții acoperă nevoile utilizatorilor individuali, dar și ale companiilor. " a declarat Attila Gömbös.

Cloud versus "on premises"

"Unul dintre obiectivele noastre este dezvoltarea unor soluții care să răspundă infrastructurii IT, care se află în plină schimbare în momentul de față. Astfel, am dezvoltat soluții precum Deep Security, care sunt apte să ofere un suport complet pe zona de securitate în mediile virtuale. De asemenea, avem soluții capabile să răspundă nevoilor unor data centere și mediilor de tip private cloud. Nu în ultimul rând, avem soluții perfect integrate cu mediile cloud de tip public Windows Azure și Amazon Elastic Cloud. În momentul de față, soluțiile noastre acoperă toate nevoile, începând cu soluții de securitate pentru servere tradiționale în regim <<on premises>>, până la soluțiile complexe disponibile în cloud. " a precizat Attila Gömbös.

Dezvoltarea rețelei de parteneri în România

Liderul mondial în soluții de securitate are un program global dedicat partenerilor, al cărui scop constă în dezvoltarea unei rețele de beneficii și competențe care să susțină dezvoltarea brandului la nivel local. După ce în luna februarie Trend Micro și Veracomp au semnat contractul de distribuție pentru Romania, au avut loc mai multe manifestări de promovare a acestui parteneriat dedicate atat channel-ului, dar si awareness-ului general – securITrends, IT out of the box-zona 9, Zcom, etc

"Ne face plăcere să lucrăm cu Veracomp pentru a îmbunătăți prezența noastră pe piața românească. Veracomp dispune de competențe și resurse pentru dezvoltarea canalului nostru de parteneri pe zona de securitate. Am înregistrat deja mai multe evoluții bune pe piața din România și considerăm că este un bun început al relației cu partenerii locali pentru soluțiile noastre." a concluzionat Attila Gömbös.

Detalii despre evenimentele Veracomp sunt disponibile aici:

http://veracomp.ro/blog/evenimente/2956-securitrends-provcare-si-oportunitate.html

http://veracomp.ro/blog/evenimente/3037-zona-9.html

SYNOLOGY DISKSTATION DS216J

În materie de echipamente NAS, cei de la Synology nu mai au nevoie de nici o introducere. Au reuşit mereu să capteze atenţia pieţei de storage oferind soluţii fiabile, performanţe şi accesibile ca preţ.

În cazul de faţă, modelul DS216j primit la teste, se adresează segmentului de consumer, fiind un mediu de stocare perfect pentru cei ce caută un home server fiabil, puteric şi eficient, atât din perspectiva performanţelor cât şi a consumului de energie.

Deşi are un design compact, DS216j vine dotat cu două bay-uri HDD de 3.5”/2.5” ce permit crearea unui spaţiu de stocare impresionant de maxim 16 TB (2x 8 TB HDD sau 1x 16 TB HDD). Vine echipat cu un procesor dual core cu motor de criptare, datorită căruia este capabil să ofere viteze de transfer de până la 112.75 MB/s la citire şi peste 97.6 MB/s, atunci când cele două HDD-uri sunt configurate în RAID.

Este destul de silenţios, oferind un nivel de zgomot sub 18.2 dB şi are un consum de invidiat, de doar doar 14.85 W în timpul utilizării şi de 6.95 W în modul de hibernare.

Din perspectiva uşurinţei în utilizare, configurarea şi integrarea sa în fluxul de lucru se face foarte uşor, urmând cei câţiva paşi menţionaţi în manual. Pentru uşurinţă în utilizare, interfaţa oferită de sistemul de operare DiskStation Manager (DSM) este una foarte simplă, ce oferă acces rapid la toate funcţiile şi opţiunile NAS-ului, precum şi la o gamă extinsă de aplicaţii.

Spre exemplu, accesând secţiunea Package Center, vei putea instala atât aplicaţii multimedia precum Audio Station, iTunes Server, Media Server, Photo Station sau Video Station, cât şi pachete software de back-up, business, supraveghere, cloud, download sau securitate.

DS216j stă bine şi la capitolul streaming video, fiind compatibil cu PC-uri, dispozitive mobile, televizoare, sau orice alte dispozitive DLNA.

Nu este un NAS foarte ieftin, dar nici unul scump dacă ţinem cont de ceea ce poate oferi.

Preţ: 839 lei pe Pcgarage - http://www.pcgarage.ro/nas/synology/diskstation-ds216j/

Apreciere ITChannel: 9/10

BENQ TH670S

BenQ a inventat modul Fotbal pentru noile proiectoare de domiciliu W1110S și TH670s, pentru ca fanii fotbalului să se simtă ca și cum s-ar afla pe stadion, luând parte la acțiune. Combinând reglarea de precizie a culorilor cu îmbunătățiri digitale, pentru tonuri ultrarealiste ale pielii și o iarbă verde abundentă, modul imagine Fotbal asigură o proiecție foarte bună, pe un ecran mare, pentru ca fiecare secundă a meciului să pară mai mare ca în realitate. În afara unor performanțe de culoare bune, realiste, proiectoarele de domiciliu BenQ sunt prevăzute cu un sistem optic optimizat 1080p Full HD pentru o claritate și detalii fără precedent ale imaginii, alături de caracteristici precum deplasarea obiectivului, proiecție laterală, tehnologie short-throw, zoom mare, precum și conectivitate wireless Full HD și o interfață prietenoasă cu utilizatorul.

Apreciere ITChannel: 10/10

Specificații:

Sistem de proiecţie	DLP 3D
Rezoluţie nativă	1080P (1920x1080) Full-IHD
Luminozitate	3,000 ANSI Lumeni
Contrast	10000:1
Culori afişate	1.07 miliarde culori

OPSWAT – SOLUȚII DE SECURITATE PENTRU SISTEMELE CRITICE

Opswat este o soluție de securitate și antivirus dedicată infrastructurilor critice (instituții guvernamentale, centrale nucleare etc.). George Prichici (Product Manager - Opswat) ne-a oferit mai multe informații despre gama de soluții a companiei.

"Gama de soluții Opswat Metadefender este dedicată companiilor care au nevoie de un grad extrem de ridicat de securitate. În prezent, majoritatea celor 160 de centrale nucleare din SUA folosesc soluția companiei. De asemenea, framework-ul antivirus este integrat în peste 90% dintre platformele distribuite de producători de top precum Cisco sau Juniper. " a precizat George Prichici (foto).

Opswat a dezvoltat una dintre cele mai performate platforme multi-scan, folosind diverse motoare antivirus. Versiunea on premises integrează peste 30 de motoare de scanare antivirus, iar versiunea în cloud un număr record de 43 de motoare de scanare.

"Țintele noastre sunt zonele de government și enterprise, precum și verticalele în care sunt necesare rețele închise. Un exemplu, este soluția de tip <<kiosk Info touch>> dedicată retelelor închise și care adresează aceste domenii. Pentru rețelele închise, în care nu este oferit acces la Internet sau la stickurile USB, soluția permite scanarea fișierelor prin intermediul info touchului și transmiterea lor în rețeaua organizațiilor. Comunicarea este unidirecțională, acest lucru asigurând un nivel ridicat de securitate. După atacurile asupra centralelor nucleare din Iran, soluția noastră s-a generalizat în acest domeniu. " a declarat George Prichici.

Soluțiile Metadefender sunt disponibile atât pe Windows, cât și pe platformele Linux. De asemenea, Opswat dispune de soluții de tip mail agent pentru serverele de mail Exchange, dar și pentru multitudinea de servere de e-mail open source.

Compania dispune de o filială de dezvoltare în România, la Timișoara, iar în prezent echipa are peste 20 de oameni. *"Este destul de greu să găsești oameni calificați pe piață, dar ne dorim extinderea echipei. "* a precizat George Prichici.

Legat de strategia companiei pe piața locală, George Prichici a declarat: *"Opswat este un nume foarte cunoscut pe piața din SUA, dar nu are aceeași notorietate pe piața locală. Pentru România, avem un parteneriat solid cu Romsym Data, firmă pentru care apreciem nivelul ridicat de know-how și conexiunile pe această piață. "*

Opswat este o companie de software cu sediul la San Francisco, care oferă soluții pentru a securiza și administra infrastructura IT. Fondată în 2002, OPSWAT dispune de tehnologii care protejează organizațiile împotriva amenințărilor și facilitează fluxul de date digitale securizate. Aplicațiile intuitive și kiturile complete de dezvoltare a lui OPSWAT sunt implementate de către IMM-uri, întreprinderi și clienții OEM la mai mult de 100 de milioane de obiective la nivel mondial.

Informații despre soluțiile Opswat:
www.romsym.ro

VIVA H701 LTE

Tableta dispune de conectivitatea 4G Dual Mode. Se pot urmări show-uri de divertisment, filme și seriale favorite sau pot fi descarcărcate cele mai recente jocuri, la viteze de download de pana la 150 Mbps. Tableta este înzestrată cu GPS, Bluetooth 4.0 și CALL Function care o transformă într-un telefon. Ecranul este IPS, fiind de foarte bună calitate.

Tableta Viva H701 LTE este echipată cu procesor Quad Core și are 1GB memorie RAM. Memoria Flash de 8GB poate fi extinsă prin adăugarea unui card microSD de până la 128GB. Dispozitivul rulează sistemul de operare Android 5.1 Lollipop, oferindu-le astfel utilizatorilor o interfață prietenoasă și intuitivă.

Considerăm că tableta prezintă un raport excelent preț/performanță.

Apreciere: 9/10

Specificații:

Conexiune 4G Dual Mode (FDD&TDD)
Functie apelare
CPU: Quad Core
GPU: Mali T720
Display 7” IPS, 1024x600 px, Full Lamination
Android™ 5.1, Lollipop
GPS
Memorie RAM 1GB
Memorie Flash 8GB
Suporta card microSD de pana la 128GB
Bluetooth, Wi-Fi Direct
Doua camere foto

PHILIPS V526

V526 este un telefon cu funcții decente, fiind propulsat de un procesor quad core la 1,3 GHz. Este Dual SIM și este înzestrat cu un ecran de 5 inch IPS la o rezoluție de 1280 x 720 pixeli. Dispune de o cameră foarte bună, pe spatele telefonului, de 13 MP. Camera web frontală este de 2 MP. Telefonul este bazat pe tehnologia X Power, având o baterie de 5000 MaH, care potrivit producătorului duce telefonul 47 de zile în stand by.

Pus în valoare de Android, telefonul dvs. mobil Philips vine echipat cu o platformă mobilă complet personalizabilă, deschisă unei game largi de aplicaţii şi funcţii inteligente. Găsiţi-vă PC-ul de buzunar, consola de jocuri şi telefonul, încorporate convenabil într-un singur dispozitiv.

Apreciere: 8/10

Specificații:

- 4G TDD, 2600 MHz, banda 38
- 3G
- Sim: Dual SIM
- Sistem operare: Android 5.1, Lollipop
- Ecran: 5” IPS
- Rezolutie ecran: 1280x720 px
- Procesor: Quad Core 1,3 GHz
- Memorie RAM: 1 GB
- Memorie internă: 8 GB
- Cameră: 13MP, Cameră frontala 2 Mp
- Altele: Bluetooth v4.0
- Baterie: 5000 mAh

INTERNET & MOBILE WORLD 2016

Join the largest B2B digital and IT solutions expo-conference in the CEE

5-6 October, Romexpo

DISCOVER THE **TECHNOLOGY** THAT WILL SHAPE **YOUR BUSINESS**

1,800+
tech solutions

120+
exhibitors

90+
sessions on digital trends

Get your limited time free pass now at
www.imworld.ro