# NOTIFICAREA VULNERABILITĂȚILOR

*Rodica Bulai, Cucu Eugeniu, David Eugeniu*
*Universitatea Tehnică a Moldovei*

***Summary:*** *This talk is about a new system that is about to be implemented by us. It will be a new approach on vulnerability monitoring that will permit to reduce the amount of work for IT professionals and will be a easy to use tool for everyone that is concerned about security of their gadgets.*

**Introducere**

Ținând cont de trendurile actuale, tot mai multe dispozitive devin „smart" și devin tot mai accesibile oamenilor de rând. Aceste dispozitive, având necesitatea de a procesa ceva informație, vin cu sisteme de operare în care sunt înscrise comenzile care urmează să le poată îndeplini, însă puține din ele sunt elaborate și optimizate pentru a oferi securitate din start. Din acest motiv, apare necesitatea de a fi mereu la curent cu ultimele noutăți din domeniul IT și în special apare necesitatea de a fi la curent cu amenințările și vulnerabilitățile noi apaărute.

Astfel, dacă până la un moment, doar cei care erau nevoiți și impuși de responsabilitățile de serviciu, analizau situația la zi și erau la curent cu cele mai noi vulnerabilități, această necesitate apare astăzi și la utilizatorii de rând care utilizează lucruri „smart" (IoT).

Pentru aceasta vin în ajutor multe portaluri de noutăți din lumea IT, multe baze de cunoștințe despre vulnerabilități au RSS feed-uri care pot fi configurate, însă o astfel de soluție presupune ca utilizatorul să filtreze informația. Din cantitatea de informație obținută, să fie capabil să depisteze doar acele amenințări care îl afectează într-o oarecare măsură. Acest lucru fiind extrem de greu de realizat, multe din amenințări având diferiți vectori de atac și realizându-se prin diferite metode, utilizând vulnerabilități ale aplicațiilor, serviciilor, sistemelor de operare sau a componentelor hardware.

În lumea IT mereu a fost și va rămâne actuală necesitatea de a fi la curent cu toate noutățile tehnologice, iar pentru ofițerii de securitate, administratorii de rețea, administratorii de sistem și alte persoane responsabile de administrarea echipamentelor, este critic de a cunoaște care pot fi amenințările și prin ce vulnerabilități acestea se pot realiza. În ajutor vin scanerele de vulnerabilități, însă acestea consumă foarte multe resurse, necesită configurare și actualizare manuală, plus la rularea unei scanări, acestea consumă foarte mult trafic și adaugă un „stres" mare pe echipamentele verificate. Din acest motiv scanerele de vulnerabilități sunt setate de a rula la o perioadă stabilită pentru a nu întrerupe activitatea afacerii. Astfel scanerele de vulnerabilități sunt o măsură de control, însă nu este suficientă, răufăcătorii fiind mereu în căutarea noilor vulnerabilități, iar în lumea IT dacă nu mergi în pas cu răufăcătorii, devii victimă.

**Sistem de notificare a vulnerabilităților**

Un sistem de notificare a vulnerabilităților vine să rezolve unele probleme discutate mai sus, și anume:

- Realizează filtrarea informației pentru utilizatori.

- Dispune de un scaner, care rulează la inițierea sistemului, și care depistează echipamentele, sistemele de operare, serviciile și aplicațiile utilizate de către deținător. Totodată, utilizatorul poate introduce manual ceea ce nu a putut depista scanerul. Astfel, sistemul deținând informații despre resursele informaționale ale utilizatorului, poate notifica utilizatorul doar despre amenințările la care sunt supuse resursele sale. Aceasta permite micșorarea semnificativă a volumului de lucru oderind un mare avantaj nu doar persoanelor entuziasmate de lumea tehnologiilor moderne, ci și administratorilor de sisteme.
- Notificarea conține nu doar date despre vulnerabilitatea nou apărută, ci și recomandări de remediere a acesteia. Acest lucru, permite iarăși micșorarea volumul de lucru care urmează să fie realizat de administratorii de sisteme, cât și asistarea persoanelor cu cunoștințe mai reduse în domeniul securității informaționale.
- Sistemul oferă posibilitatea de a genera rapoarte, ceea ce poate fi util pentru utilizatori de rând și foarte util pentru administratori de sisteme. Rapoartele fiind personalizabile, oferă posibilitatea de a selecta ce informații să fie incluse și în ce format generate.
- Sistemul utilizează cele mai cunoscute și avansate baze de cunoștințe cu vulnerabilități: Exploit Database (exploit-db), National Vulnerability Database (NVD), CVESecurity Vulnerability Database și Rapid7 Vulnerability Database. Aceste baze de cunoștințe dețin informații despre vulnerabilități deja existente și sunt actualizate regulat cu noi vulnerabilități, datorită cooperării cu echipe de cercetare din domeniul securității informaționale.
- Datorită faptului că sistemul nu are necesitatea de a scana permanent rețeaua pentru depistarea vulnerabilităților, acesta nu consumă resurse, iar posibilitatea de a introduce manual date despre resurse informaționale oferă flexibilitate înaltă de întreținere și actualizare.

Sistemul conține o aplicație client prin care utilizatorii pot configura notificările și un API prin care sistemul poate fi integrat cu alte soluții proprii. Notificările despre vulnerabilități pot fi primite în cadrul aplicației client sau să fie expediate pe adresa de email a utilizatorului, figura 1.

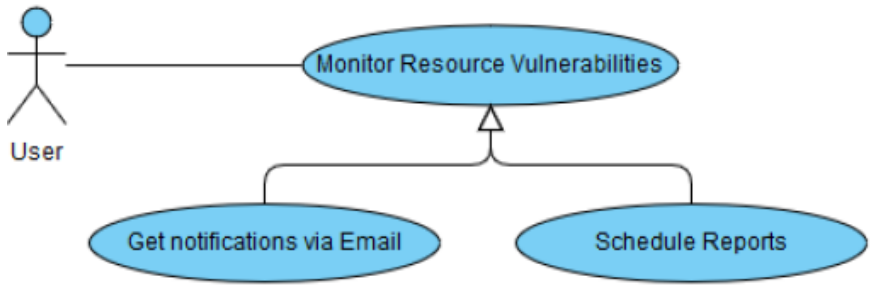


***Figura 1* – Diagramă generală de caz utilizare**

Aplicația este proiectată pentru a fi simplă în utilizare atât de profesionaliști din domeniul IT, cât și de utilizatorii de rând, iar API-ul poate fi de mare folos pentru întreprinderile care doresc să dezvolte propriile soluții sau doresc să integreze soluția dată cu alte proiecte.

Aplicația client poate fi utilizată pe mai multe platforme cur ar fi: platforma mobilă (Android, iOS), platforma desktop (Mac, Linux, Windows), sau pe platforma web. Acest lucru este posibil prin API GATEWAY care servește ca punct unic de intrare în aplicație și care comunică la fel cu toate platformele utilizând un API specific pentru fiecare din platforme, figura 2.

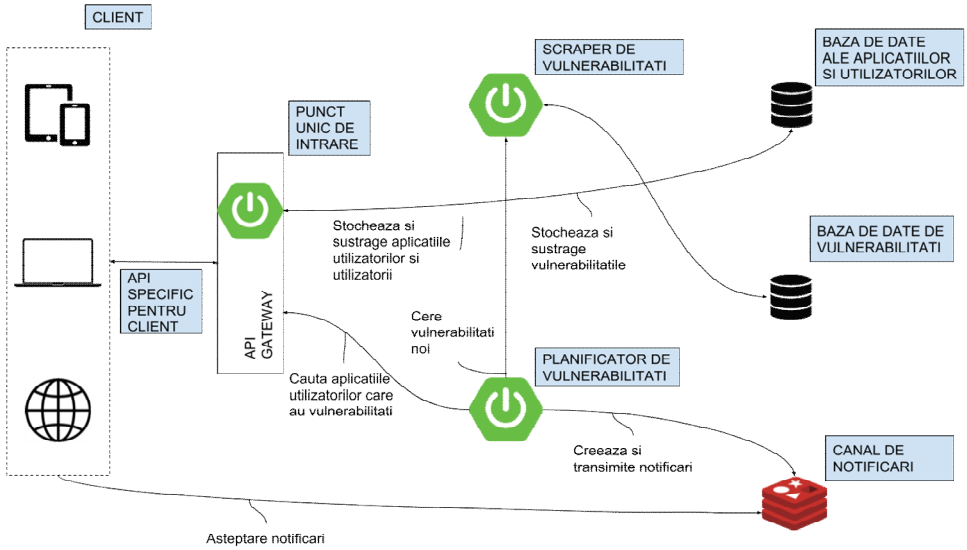


***Figura 2* – Diagrama comportamentală a sistemului**

Conform figurii 2 se poate de observat că în calitate de CLIENT poate fi utilizat orice dispozitiv pe orice platformă, client-ul comunicând cu API GATEWAY utilizând un API specific pentru fiecare platforma.

Clientul ce comunică cu API-ul poate înregistra aplicațiile sale în BAZA DE DATE DE APLICATII ŞI UTILIZATORI, după care primește o cheie unică pentru CANALUL DE NOTIFICARI de unde va primi notificarile.

La aceasta etapa acțiunile utilizatorului se încheie, și urmează partea de procesare a vulerabilităților de servicii PLANIFICATOR DE VULENERABILITĂȚI și SCRAPER DE VULNERABILITĂȚI, care găsind vulnerabilități noi le stochează în BAZA DE DATE DE VULNERABILITĂȚI, apoi găsind aplicațiile vulnerabile costruiește notificari și le transmite în canalul de notificări.

Cu toate că pe piață deja există unele soluții care oferă notificări despre vulnerabilități, acestea vin în formă de noutăți săptămânale sau la intervale stabilite de utilizator. De asemenea, informația expediată de aceste soluții nu poate fi filtrată ușor. De exemplu, *US-CERT Alarms* nu oferă nici un criteriu de filtrare, informația primită de

utilizator, cuprinde toate vulnerabilitățile noi apărute pe perioada stabilită. O altă soluție existentă, *CVE Details Vulnerability Feeds & Widgets*, oferă niște criterii de filtrare a informației, însă aceasta se limitează la tipurile de vulnerabilități și nu șa platforme, sisteme de operare sau servicii. Iar soluția *Secunia*, este una cu funcțional mai vast, pe lângă notificări, oferind suport tehnic și consultații și este o soluție contra plată orientată spre specialiștii în domeniul securității informației și infrastructuri ale companiilor IT.

**Concluzii**

Soluția dezvoltată și descrisă în acest articol vine ca un instrument potrivit pentru a asigura securitatea echipamentelor atât personale, pentru utilizatori de rând, cât și infrastructuri IT din cadrul întreprinderilor. Funcționalitățile oferite de sistem asigură notificarea în cel mai scurt timp despre noile amenințări, ceea ce poate fi critic în unele situații.

Tot odată, acest instrument nu consumă resurse și nu împiedică în nici un fel activitățile echipamentelor IT. Datorită faptului că utilizatorul introduce în sistem denumirea echipamentelor/aplicațiilor/SO-urilor deținute și versiunile acestora, soluția filtrează informația care urmează să fie expediată, ceea ce ușurează substanțial lucrul cu sistemul dat.

Sistemul oferă un API care permite încorporarea funcționalului în alte aplicații sau sisteme, acest lucru fiind un mare avantaj pentru companiile care au nevoie să modifice sau să adauge ceva componente, care să corespundă necesităților acestora.

**Bibliografie:**

1. Information security (infosec), Margaret Rouse - http://searchsecurity.techtarget.com/definition/information-security-infosec
2. Exploit Database - https://www.exploit-db.com/
3. National Vulnerability Database - https://nvd.nist.gov/
4. CVESecurity Vulnerability Database - https://www.cvedetails.com/
5. Rapid7 Vulnerability Database - https://www.rapid7.com/db