Principiile fundamentale ale securității cibernetice

în procesul de testare software

Prezentul raport are la bază articolul publicat de [**Ivanchenko Yevhenii**](https://inlibrary.uz/index.php/index/search?query=Ivanchenko%20Yevhenii) în 21.04.2025 **Fundamental Principles of Cybersecurity in The Software Testing Process,** privind examinarea principiilor asigurării securității cibernetice în timpul testării software-ului. În ultimul timp s-a ajuns la concluzia că testarea software nu este indicat să fie limitată doar la verificări de validare, ci să incorporeze și evaluarea riscurilor, în conformitate cu standardele actuale, dar și o analiză a slăbiciunilor în stadiile incipiente ale dezvoltării aplicațiilor.

Dezvoltarea digitalizării din ultimul timp a dus la o creștere majoră a atacurilor cibernetice, în 2024 creșterea a fost de 46% față de 2023[[1]](#footnote-1). Lunar sunt blocate peste 1 miliard de amenințări cibernetice, iar analiștii au ajuns la concluzia că 95% dintre atacuri sunt efectuate prin motoarele de căutare[[2]](#footnote-2).

Aceste statistici au dus la concluzia că testarea software este extrem de importantă, ajutând la identificarea și remedierea timpurie a breșelor înainte ca produsul să fie dat spre utilizare. În afară de aspectele tehnice, securitatea informațiilor legale și de conformitate este foarte importantă: GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST, etc.

Literatura de specialitate evidențiază legătura dintre conformitate și securitate (ex. Folorunso A. et al.), importanța adaptării standardelor internaționale (ex. Carter W. A. și Crumpler W. D.), dar și lipsa unor modele clare pentru integrarea securității în testarea software (ex. Hamdani S. W. A. și Kaplan B., Williams B. și Adamson J.). Sunt analizate contribuții privind utilizarea inteligenței artificiale (ex. Machireddy J. R., Mohamed S. A.), automatizării și cultura organizațională pentru creșterea securității (ex. Alshaikh M.).

Un domeniu distinct este cel al sistemelor ciber-fizice, unde se propune o abordare mixtă de testare și analiză a riscurilor, cu aplicabilitate în sectorul energetic(ex. Zografopoulos I. și alții).

Se identifică o lacună importantă în integrarea directă a cerințelor de securitate în procesele de testare software. Este necesară o abordare sistematică în care securitatea cibernetică este parte integrantă a testării, cu roluri clar definite și coordonare între testeri și experții în securitate, această integrare crește randamentul software-ului și eficiența detectării breșelor.

1. **Rolul principiilor de securitate cibernetică în conturarea strategiilor de testare**

Standardele moderne de securitate (precum GDPR, HIPAA, PCI DSS, ISO/IEC 27001, NIST) influențează direct procesul de dezvoltare software, inclusiv testarea. O abordare eficientă presupune integrarea cerințelor de securitate încă din fazele de design și testare, nu doar ca un control final de calitate. În lipsa unor principii clare și a unei supravegheri constante, testarea poate omite aspecte critice de securitate, ducând la aplicarea selectivă a măsurilor de protecție.

Este esențială elaborarea unei strategii unificate de testare care să includă cerințele specifice fiecărui domeniu de activitate (PCI DSS în sectorul financiar, HIPAA în sănătate, etc.) și să definească clar responsabilitățile echipelor implicate: cine configurează, controlează accesul, auditează etc. Documentarea riguroasă și transparența procesului întăresc credibilitatea și eficiența în răspunsul la incidente. Un alt rol crucial în dezvoltarea unei culturi organizaționale de securitate matură este jucat de formarea profesională.

Un model eficient de testare integrează cerințele de reglementare în toate scenariile de testare și se bazează pe:

* + Evaluarea vulnerabilităților arhitecturii aplicației.
  + Protecția datelor în timpul transmisiei și stocării.
  + Identificarea slăbiciunilor în autentificare și autorizare.
  + Verificarea utilizării și securității fișierelor de jurnal.

Tabelul de mai jos prezintă un exemplu al influenței diferitelor principii de securitate cibernetică asupra strategiei de testare.

|  |  |  |
| --- | --- | --- |
| **Regulator/Standard** | **Key Cerințe de securitate** | **Impact asupra**  **strategiei de testare** |
| GDPR | Protecția datelor personale, notificarea incidentelor, dreptul la ștergerea datelor | Testarea procesării datelor personale (inclusiv anonimizarea), verificarea ștergerii/actualizării corecte a datelor, auditarea jurnalelor pentru conformitate cu cerințele de confidențialitate |
| HIPAA | Securitatea informațiilor medicale, confidențialitatea, responsabilitatea | Modelarea scenariilor de scurgere a PHI (Informații medicale protejate), verificarea criptării, auditarea drepturilor de acces pentru datele pacienților, testarea procedurilor de oprire de urgență. |
| PCI DSS | Protecția datelor de plată, segmentarea rețelei, monitorizarea tranzacțiilor | Testarea la stres sub sarcini mari, verificarea criptării, verificările stocării datelor de pe card, analiza istoricului tranzacțiilor, testarea firewall-ului și a detecției de intruziune. |
| ISO/IEC 27001 | Managementul cuprinzător al securității, îmbunătățirea continuă a proceselor. | Dezvoltarea unui sistem de audit pentru testare, teste de penetrare regulate, documentarea politicilor de gestionare a incidentelor, integrarea unei abordări bazate pe risc. |
| Cadru de securitate cibernetică NIST | Identificare, protecție, detectare, răspuns, recuperare | Modelare a amenințărilor, dezvoltarea planului de răspuns, analiza rezilienței în cazul defecțiunilor, aplicarea instrumentelor CI/CD pentru monitorizarea continuă a securității |

Conform tabeului de mai sus, standardele și cadrele de reglementare impun cerințe de securitate care influențează direct scenariile de testare. Integrarea verificărilor pentru protecția datelor, disponibilitatea resurselor și răspunsul la incidente consolidează reziliența cibernetică a produsului. Principiile de securitate devin astfel un cadru fundamental în planificarea și executarea testelor, ajutând la prevenirea vulnerabilităților critice și la adaptarea rapidă la schimbări. Această abordare transformă securitatea într-o componentă esențială a întregului proces de testare, nu doar într-un pas final.

1. **Principiile cheie de cibersecuritate în testare**

Aplicarea principiilor fundamentale de cibersecuritate în testarea software permite identificarea și atenuarea riscurilor înainte de implementare. O abordare bazată pe risc prioritizează testarea componentelor critice, în funcție de impactul și probabilitatea amenințărilor, fiind susținută de o reevaluare continuă pe măsură ce sistemul evoluează.

Triada confidențialitate-integritate-disponibilitate (CIA) ghidează testarea în medii reglementate. Protecția datelor impune anonimizare, criptare și control al accesului, conform cerințelor ca GDPR și HIPAA. Integritatea este asigurată prin validări cu valori hash și instrumente de analiză integrate în procesele CI/CD. Disponibilitatea este testată prin simulări de sarcină, testare de failover și exerciții de recuperare în caz de dezastru, garantând funcționarea serviciilor critice în orice condiții.

Tabelul 2 de mai jos descrie modul în care sunt aplicate principiile triadei CIA în scenariile de testare.

|  |  |  |
| --- | --- | --- |
| **Măsuri** | **Cheie de principiu** | **Exemple de scenarii de test** |
| Confidențialitate | -anonimizarea datelor/pseudonimizarea - Criptarea datelor în repaus și în tranzit  - Controlul accesului bazat pe roluri | 1. Înlocuirea datelor de test pentru a exclude identificatorii personali pentru inginerii QA.  2. Verificarea certificatelor TLS/SSL și a mecanismelor de criptare.  3. Asigurarea că numai personalul autorizat are acces la datele sensibile. |
| Integritate | - Controlul versiunilor și validarea hash-urilor  -Managementul configurației  – Analiza statică și dinamică a codului | 1. Compararea valorilor hash înainte și după modificările bazei de date.  2. Rularea instrumentelor SAST/DAST pentru a detecta injecții de cod nesigure.  3. Testarea procedurilor de revenire pentru instalările defectuoase de patch-uri. |
| Disponibilitate | - Testarea încărcăturii și a stresului  – Teste de failover și recuperare în caz de dezastru  –Monitorizarea consumului de resurse | 1. Simularea traficului de vârf pentru a măsura timpul de răspuns (Testarea încărcăturii).  2. Oprirea unui server dintr-un cluster pentru a valida failover-ul automat.  3. Analizarea jurnalelelor în timpul unor creșteri neobișnuite ale utilizării resurselor (Scenarii de atac DoS). |

Integrarea automatizării și a tehnologiilor moderne în testarea securității cibernetice reduce sarcinile repetitive și îmbunătățește eficiența proceselor de conformitate. Instrumentele automate colectează și analizează în timp real rezultatelor testelor și statisticilor de vulnerabilitate, generează rapoarte de conformitate, ex. GDPR, PCI DSS, și monitorizează continuu configurările sistemului, cu alerte de erori.

În cadrul DevOps, verificările automate de securitate sunt integrate în pipeline-urile CI/CD, iar roboții RPA contribuie la validarea setărilor și trimiterea rapoartelor către sistemele SIEM. Algoritmii de învățare automată și inteligență artificială facilitează detectarea anomaliilor, generează scenarii de testare adaptate cerințelor (ex: GDPR, HIPAA) și actualizează testele în funcție de noile vulnerabilități.

Tehnologii precum containerizarea și analiza compoziției software (SCA) completează acest ecosistem, asigurând respectarea standardelor de securitate în toate etapele dezvoltării.

Tabelul 3 oferă o privire de ansamblu asupra instrumentelor de automatizare utilizate frecvent în testare, împreună cu funcționalitățile lor.

|  |  |  |
| --- | --- | --- |
| **Instrument/Program** | **Functia principala** | **Aplicația de Conformitate** |
| SAST/DAST (e.g.,  SonarQube, OWASP ZAP) | Analiza statică și dinamică a codului, detectarea vulnerabilităților | Identifică riscurile de codare și exploatare relevante pentru PCI DSS, HIPAA, GDPR etc. |
| SIEM Systems (e.g., Splunk, QRadar) | Colectarea și corelarea jurnalelor de evenimente de securitate, detectarea anomaliilor | Generarea automată a rapoartelor de conformitate (ISO/IEC 27001), alertare în timp real pentru incidente de securitate |
| RPA (de exemplu, UiPath, Automation Anywhere) | Emularea acțiunilor utilizatorului/sistemului, integrarea cu servicii externe, | Automatizează comparațiile de rutină între parametrii actuali ai sistemului și setările de bază pentru audit și conformitate reglementară. |
| Platforme ML (de exemplu, TensorFlow, PyTorch cu module de analiză a jurnalelor) | Instruire pe date istorice, predictia comportamentului, detectia anomaliilor. | Detectarea timpurie a posibilelor scurgeri sau atacuri, alerte proactive și generarea inteligentă a cazurilor de test. |
| SCA (Analiza Compoziției Software-ului) (de exemplu, Snyk, WhiteSource | Scanarea vulnerabilităților dependențelor și bibliotecilor | asigură actualizări regulate ale componentelor pentru a respecta PCI DSS și ISO/IEC 27001, simplificând pregătirea auditului de conformitate. |

Integrarea automatizării în procesele de testare crește eficiența în identificarea abaterilor de conformitate și îmbunătățește supravegherea securității. Utilizarea tehnologiilor și cloud le întărește și mai mult această abordare, permițând diagnostice inteligente. Aceste progrese contribuie la formarea unui ciclu de îmbunătățire continuă, în care fiecare deviație detectată de la standardele de securitate devine un motor pentru rafinarea strategiilor de testare și creșterea nivelurilor de conformitate.

Studiul arată că nivelul de securitate al software-ului depinde de integrarea completă a principiilor de securitate cibernetică în testare. Doar respectarea formală a reglementărilor nu este suficientă. O abordare bazată pe risc, aplicarea triadei CIA și automatizarea testării cu instrumente moderne (CI/CD, SIEM, ML) asigură detecția timpurie a amenințărilor și o mai bună rezistență cibernetică. Evaluările periodice și îmbunătățirea continuă a politicilor sunt esențiale.

**Bibliografie:**

1. [Fundamental Principles of Cybersecurity in The Software Testing Process | The American Journal of Engineering and Technology](mailto:Fundamental%20Principles%20of%20Cybersecurity%20in%20The%20Software%20Testing%20Process%20|%20The%20American%20Journal%20of%20Engineering%20and%20Technology) by [**Ivanchenko Yevhenii**](https://inlibrary.uz/index.php/index/search?query=Ivanchenko%20Yevhenii) ([yevhenii@theamericanjournals.com](mailto:yevhenii@theamericanjournals.com)), on 21.04.2025 - https://inlibrary.uz/index.php/tajet/article/view/80559

2. [Cyberattacks to Increase 46% by 2024 | CoinsPaid Media](https://coinspaidmedia.com/news/cyberattacks-increase-46-2024) - https://coinspaidmedia.com/news/cyberattacks-increase-46-2024

1. [Cyberattacks to Increase 46% by 2024 | CoinsPaid Media](https://coinspaidmedia.com/news/cyberattacks-increase-46-2024) [↑](#footnote-ref-1)
2. [Cyberattacks to Increase 46% by 2024 | CoinsPaid Media](https://coinspaidmedia.com/news/cyberattacks-increase-46-2024) [↑](#footnote-ref-2)