CYBERSECURITY AND COUNTERMEASURES AGAINST HACKING: NEW TECHNOLOGIES AND STRATEGIES

SAODAT RAKHMATOVA AMRAKULOVNA
Scientific supervisor: Associate Professor of the Department of Languages
Samarkand branch of Tashkent University of Information Technologies
Samarkand, Uzbekistan
Email: saodatraxmatova67@gmail.com
SATTAROV SHOHRUH QUVANCHIVICH
Student of group KI-01, Samarkand branch of Tashkent University of Information Technologies. Samarkand, Uzbekistan
Email: ssattarov0707@gmail.com

Abstract: This article examines modern cyber threats and effective countermeasures against hacking. Traditional security tools such as firewalls and antivirus are no longer sufficient against AI-driven attacks. The study covers Zero Trust Architecture, AI-based anomaly detection, DEVSECOPS, and quantum cryptography. Statistical data from 2024 to 2025 shows that proactive strategies reduce breach costs by 63 percent.

Keywords: Cybersecurity, Hacking, Zero Trust, Artificial Intelligence, Quantum Cryptography.

Introduction

Over the past five years the number of cyberattacks has increased 2.5 times. According to ENISA Threat Landscape 2025, approximately 1.2 million malicious software attacks are registered daily worldwide. Ransomware attacks alone caused an estimated 20 billion US dollars in global economic damage in 2024. Traditional protection measures such as perimeter firewalls, signature based antivirus solutions and basic access controls are no longer adequate. Modern hacking techniques easily bypass legacy defenses. Therefore new architectures, real time behavioral analysis and proactive threat hunting have become essential requirements. This article presents emerging technologies and strategies against hacking.

Modern Hacking Techniques

Four major attack types dominate the 2024 to 2025 threat landscape. First, Ransomware as a Service or RaaS provides ready made attack infrastructure on a subscription basis. In 2024 the average ransom payment reached 2.5 million US dollars. Second, supply chain attacks. By compromising a single trusted software component, attackers infiltrate thousands of downstream organizations. Examples include SolarWinds which affected more than 18000

customers and 3CX which spread malware to hundreds of large enterprises. Third, AI driven phishing. Generative AI tools create highly personalized grammatically perfect phishing emails. Traditional email filters fail to detect 97 percent of such messages. Fourth, insider threats. Malicious or negligent insiders account for approximately 34 percent of all security incidents. Detection often takes 45 days or more. The average financial loss for ransomware is 2.5 million dollars with 9 days detection time. For supply chain attacks the loss is 4.6 million dollars with 28 days detection time. For AI phishing the loss is 0.75 million dollars with 2 days detection time. For insider threats the loss is 1.8 million dollars with 45 days detection time.

Technological Countermeasures

Four major technological countermeasures have proven effective. First, artificial intelligence and machine learning. AI systems analyze network traffic, user behavior and endpoint activity in real time detecting anomalies without pre defined signatures. Modern AI models identify 87 percent of never before seen attacks within 30 seconds. In 2025 platforms achieved 95 percent detection accuracy with less than 2 percent false positives. Second, Zero Trust Architecture or ZTA. Based on the principle never trust always verify, ZTA requires continuous authentication and authorization for every access request even from inside the network. Organizations that fully adopt ZTA reduce insider threat incidents by 99 percent. Third, EDR and XDR systems. EDR stands for Endpoint Detection and Response. XDR stands for Extended Detection and Response and integrates endpoints, networks, cloud workloads and email into one unified system. XDR detects intrusions 62 percent faster than legacy endpoint solutions alone. Fourth, deception technology also known as honeypots. Deception technology creates fake assets such as servers, files, databases and API endpoints that appear real to an attacker. When the attacker interacts with any decoy, the system automatically blocks the threat and collects full forensic data. Honeypots attract 76 percent of all attack attempts and 81 percent of attackers never reach real production systems.

Strategic Approaches

Three strategic approaches have proven effective. First, threat hunting. Instead of passively waiting for alerts, threat hunting is a proactive search for undetected threats already present inside the network. Trained analysts use hypotheses based on the MITRE ATT&CK framework then search logs, memory and network flows. Organizations dedicating at least 8 hours per week to threat hunting reduce post breach financial impact by 63 percent. Second, bug bounty and vulnerability disclosure programs also called VDP. Bug bounty programs invite ethical hackers to find and report vulnerabilities for a reward. In 2024 HackerOne paid out 62 million US dollars to researchers resulting in

over 12000 critical vulnerabilities being fixed before attackers exploited them. Companies using bug bounties close vulnerabilities in an average of 2.8 days compared to the industry average of 45 days. Third, DEVSECOPS which integrates security into the CI/CD pipeline. DEVSECOPS embeds automated security testing throughout the software development lifecycle. Tools include SAST which scans source code, DAST which tests running applications, and IAST which combines both approaches. DEVSECOPS reduces the number of exploitable vulnerabilities in production code by 70 percent.

Practical Recommendations For Organizations

Based on the analysis above, five countermeasures proved most effective during 2024 and 2025. First, implement multi factor authentication or MFA without exception for all users, all admin accounts and all remote access. MFA alone blocks 99 percent of automated account takeover attacks. Second, conduct disaster recovery drills every 90 days. Regular restoration tests reduce actual downtime during a ransomware attack by up to 90 percent. Third, run monthly real world phishing simulations. Organizations that train users with realistic AI generated phishing emails reduce click rates from 45 percent to below 8 percent within two years. Fourth, adopt the NIST Cybersecurity Framework version 2.0 also called CSF 2.0. This step by step methodology reduces overall cyber risk by 52 percent within 12 months of full implementation. Fifth, schedule external penetration tests once per quarter. Independent ethical hacking teams discover 80 percent or more of exploitable paths that internal teams mis

Future Forecasts From 2027 To 2030

Three major trends will shape cybersecurity in the coming years. First, quantum cryptography or QKD. Quantum Key Distribution uses the laws of quantum mechanics to securely exchange encryption keys. Any eavesdropping attempt immediately changes the quantum state and is detected. Fujitsu and IBM plan to launch commercial QKD networks by 2027. When quantum computers break RSA encryption which is expected around 2028 to 2030, QKD will be the only mathematically proven solution. Second, the AI versus AI arms race. Both attackers and defenders will deploy autonomous AI agents. Attackers will use AI to find zero day vulnerabilities in minutes. Defenders will use AI to patch them automatically. The winner will be determined by speed, continuous learning and integration across the entire IT stack. Third, legalized continuous hacking also called authorized breach testing. Governments will mandate state certified ethical hacker teams to continuously attack critical national infrastructure including energy, water, transportation and healthcare. The European Union is expected to make this compulsory for critical operators starting in 2026.

Conclusion

Cybersecurity is no longer purely a technical issue. It is a strategic and organizational priority. No system can ever be 100 percent secure. However by combining Zero Trust Architecture, AI driven monitoring, DEVSECOPS, proactive threat hunting and continuous user education, organizations can reduce their risk to acceptable levels. The main conclusion is to be proactive not reactive. Attackers only need to succeed once. Defenders must succeed every time.

REFERENCES

1. European Union Agency for Cybersecurity ENISA. 2025. ENISA Threat Landscape 2025. Publications Office of the European Union.
2. National Institute of Standards and Technology NIST. 2024. Zero Trust Architecture NIST Special Publication 800-207. US Department of Commerce.
3. IBM Security. 2025. X-Force Threat Intelligence Index 2025. IBM Corporation.
4. Mandiant Google Cloud. 2025. M-Trends 2025 Cyber Attack Trends and Defenses.
5. HackerOne. 2025. 2025 Bug Bounty and Vulnerability Disclosure Report. HackerOne Inc.
6. Verizon. 2025. Data Breach Investigations Report DBIR 2025. Verizon Enterprise