The cyber threat landscape part 4: Emerging technologies and their security implications

BY INTIGRITI · NOVEMBER 27, 2024 · LAST UPDATED ON APRIL 28, 2025

As organizations continue adopting emerging technologies, they gain immense benefits but also face new security challenges. Cloud computing, AI, IoT, and blockchain are reshaping the cyber threat landscape, introducing powerful tools for defenders along with vulnerabilities for attackers to exploit. In this post, we explore how these technologies impact cybersecurity, the unique risks they bring, and best practices for mitigating those risks.

The double-edged sword of emerging technologies

While innovations like artificial intelligence (AI), the Internet of Things (IoT), blockchain, and quantum computing offer unmatched potential for business transformation, they also expand the attack surface and create unforeseen vulnerabilities. To navigate this complex terrain, organizations need to understand not only how these technologies enhance efficiency but also how they may open doors to malicious actors.

1. Artificial Intelligence (AI): Redefining both attack and defense

AI continues to revolutionize many things, including cybersecurity, helping organizations analyze vast amounts of data to identify threats and anomalies. Machine learning algorithms can identify patterns indicative of cyberattacks, allowing teams to respond faster than ever. However, attackers can also use AI to their advantage. AI-enabled cyber threats include:

- **Automated Phishing**: AI can be used to generate realistic phishing emails, social engineering content, and chatbots that mimic human behavior to deceive users.
- **Deepfake Technology**: Deepfake videos and audio clips are being used to impersonate executives in social engineering attacks, allowing attackers to bypass traditional verification methods.
- **AI-Powered Malware**: Malicious actors are developing adaptive malware that can evade detection by continuously modifying its code based on AI-driven analysis of common security defenses.

In this landscape, the use of AI-powered defenses, such as anomaly detection and predictive analytics, has become essential. However, staying vigilant about AI's potential misuse is equally important to safeguard against threat actors who might use these very tools against us.

2. IoT (Internet of Things): Expanding the attack surface

IoT devices are becoming pervasive in homes, workplaces, and critical infrastructure systems. With billions of IoT devices now online, they significantly expand the attack surface and increase potential entry points for cybercriminals. Common IoT vulnerabilities include:

- **Insecure Device Designs**: Many IoT devices lack fundamental security features, such as regular patching, robust authentication, and encrypted communication.
- **Botnets and DDoS Attacks**: Compromised IoT devices can be grouped into botnets, launching massive Distributed Denial of Service (DDoS) attacks that overwhelm networks. The Mirai botnet attack demonstrated this risk by exploiting vulnerabilities in IoT devices to shut down major online services.
- **Weak Authentication Protocols**: Many IoT devices have default, weak passwords, allowing easy access for attackers if users don't change these settings.

To secure IoT deployments, organizations should implement rigorous device management policies, such as enforcing strong passwords, securing firmware, and isolating IoT networks from critical infrastructure systems.

3. Cloud computing: Balancing accessibility and security

Cloud adoption continues as organizations seek flexibility, scalability, and cost-efficiency. However, the cloud introduces unique security concerns due to shared infrastructure, complex configurations, and the potential for misconfigured settings. Key cloud vulnerabilities include:

- **Data Exposure**: Misconfigured access permissions can leave sensitive data publicly accessible, as seen in many high-profile cloud breaches.
- **Weak Access Controls**: Cloud-based applications are often accessed from various locations and devices, making it essential to use strong identity and access management (IAM) policies.
- **Third-Party Dependencies**: Many cloud applications rely on third-party tools and APIs, creating potential risks through the supply chain.

To protect cloud environments, organizations should adopt a comprehensive cloud security posture management (CSPM) approach, ensuring continuous monitoring for misconfigurations, enforcing the principle of least privilege, and routinely auditing access controls.

4. Blockchain: Promising security, but not invulnerable

Blockchain is often touted for its security and transparency, offering a decentralized ledger system that enhances trust in data integrity. However, there have been dozens of high-cost breaches already. Blockchain technology presents specific risks that require consideration:

- **Smart Contract Vulnerabilities**: Smart contracts—self-executing contracts coded into blockchain platforms—are vulnerable to bugs and flaws. If a smart contract has an error, it could be exploited to manipulate funds or data.
- **51% Attacks**: In smaller blockchain networks, attackers who control the majority of mining power can rewrite transaction history, enabling double-spending and other fraudulent activities.
- **Privacy Risks**: Public blockchains make transactions visible to anyone on the network, which could expose sensitive data if not properly anonymized.

To mitigate blockchain-related risks, organizations should conduct smart contract audits, use secure coding practices, and ensure network decentralization to avoid control by any one actor.

5. Quantum computing: The future threat to encryption

While quantum computing remains in its early stages, its potential impact on cybersecurity is significant. Quantum computers are expected to outperform classic computers in solving complex problems, such as factoring large prime numbers—a basis for current encryption methods. Key security implications include:

- **Encryption Vulnerabilities**: Quantum computing could break widely-used encryption algorithms like RSA and ECC, rendering existing encrypted data vulnerable to decryption.
- **Future-Proofing Data Security**: Organizations need to prepare for a post-quantum era by adopting quantum-resistant encryption methods as they become available.
- **Data Retention Risks**: Sensitive data encrypted with current standards but stored for long periods could eventually be decrypted if quantum computing advances.

Although practical quantum computing attacks are still years away, organizations should track developments in quantum-safe encryption algorithms and consider adopting them as part of a long-term data protection strategy.

The creativity of cyber threat actors: Beyond traditional methods

Emerging technologies also amplify the creativity of attackers, who consistently push boundaries to exploit weaknesses. One example that underscores this creativity is the use of 3D printing technology by hackers to create highly realistic facial masks. These masks can trick biometric authentication systems like face recognition on laptops or smartphones, enabling unauthorized access. By leveraging 3D printed models based on images or data from social media, attackers can bypass face ID systems with surprising accuracy. This tactic highlights the innovative—and often unpredictable—methods that threat actors use to manipulate security technologies designed to protect.

To counter these risks, organizations should incorporate multi-factor authentication (MFA) and consider additional security layers for sensitive devices. Recognizing the adaptability of attackers underscores the need for vigilance in defending against both conventional and unconventional threats.

In addition, bug bounty programs offer a proactive solution to combat the ingenuity of threat actors. By incentivizing ethical hackers from around the globe to identify vulnerabilities, organizations can tap into a diverse pool of creative minds to outmaneuver attackers. Leveraging such a wide pool of security expertise creates a dynamic defense strategy that matches—and often exceeds—the innovative tactics employed by cybercriminals.

Safeguarding against technology-driven vulnerabilities

With each new technology, organizations need to strike a balance between embracing innovation and ensuring security. The following best practices can help secure emerging technologies effectively:

1. **Adopt a Multi-Layered Defense Strategy**: A comprehensive security framework that includes monitoring, access control, and incident response can minimize vulnerabilities, especially with

interconnected IoT devices and cloud services.

2. **Regularly Update and Patch**: Frequent updates and patches for IoT devices, cloud applications, and other tech components are essential to avoid known vulnerabilities.
3. **Use AI and Machine Learning Defensively**: Leverage AI for threat detection and behavior analysis, enabling faster responses to novel attack vectors. However, monitor and verify AI use to avoid automation bias and false positives.
4. **Strengthen Access Controls and Authentication**: Implementing strong authentication measures, such as multi-factor authentication (MFA), can help prevent unauthorized access in cloud and IoT environments.
5. **Prepare for Quantum Resilience**: As quantum technology advances, begin exploring quantum-resistant encryption options to protect data and future-proof organizational security.
6. **Leverage Bug Bounty Programs**: Bug bounty programs harness the creativity of a global community of ethical hackers to identify vulnerabilities before they can be exploited by threat actors. By incentivizing proactive vulnerability discovery, bug bounty programs serve as a critical component of a dynamic and adaptive defense strategy.

Conclusion: Balancing innovation and security

Emerging technologies offer tremendous potential to drive efficiency and enable growth, but they also introduce unique and evolving cybersecurity risks. By understanding these technologies' benefits and vulnerabilities, organizations can proactively secure their environments and protect against emerging threats.

In the final part of this series, we'll discuss how organizations can develop a mature, multi-layered cybersecurity strategy to maintain resilience in an ever-shifting threat landscape.

In the meantime, if you'd like to speak with one of our experts to understand if bug bounty could be right for you, get in touch today.