NEXSAN
A StorCentric Company

THE LIFECYCLE OF A CYBERATTACK

THE INCREASED THREAT OF ATTACK FACTS AND FIGURES

- **65 percent of cyber threats** go undetected
- Data breaches usually last, on average, **280 days** before they are uncovered
- The average recovery cost associated with a data breach is **$4.24 million**
- There were **5.4 billion logged attempted malware attacks** in 2021 and 623.3 million attempted ransomware attacks

Cyberattacks are all too common, and they place companies in jeopardy. A cyberattack happens every 39 seconds somewhere online. The first step to being prepared is understanding how these attacks happen.

HOW CYBERATTACKS HAPPEN

1. External Reconnaissance: Malicious actors research their target, identifying system vulnerabilities, users to attack, and specific approaches they believe will be successful. This includes public-facing apps and services, as well as individuals to exploit.

2. Primary Compromise: The cybercriminals execute some kind of malicious code, either through social engineering attempts like phishing, taking advantage of a vulnerability in the network, by brute force, or by some other means.

3. Internal Reconnaissance: The attacker gathers information about the network environment, learning the roles and responsibilities of important individuals, and locating where sensitive, valuable, or confidential information is stored.

4. Expansion & Escalation: Following the initial compromise, attackers expand their presence and escalate privileges to take over the system. This can be done in a myriad of ways, including exploiting credentials, misconfigurations, vulnerabilities, or through social engineering.

5. Exfiltration: Once the attacker has control over the compromised environment, they can move from place to place, accessing network shares, using remote access tools, and targeting specific systems, data pools, and more to extract sensitive data.

6. Complete the Attack: After achieving their intended goal, like stealing intellectual property, sensitive or confidential data, or personally identifiable information, many cybercriminals maintain access for potential future missions.

THE RISING RISK OF STATE-SPONSORED CYBER CRIME

Independent research shows a **100% rise in "significant" nation-state incidents** from 2017 to 2020. An analysis of 200 incidents of nation-state related attacks found that **the most common targets** were:

- Enterprises received 35% of attacks
- Cyberdefense received 25% of attacks
- Media and communications received 14% of attacks
- Government bodies and regulators received 12 percent of attacks
- Critical infrastructure received 10 percent of attacks

> *Nation states are devoting significant time and resources to achieving strategic cyber advantage to advance their national interests, intelligence gathering capabilities, and military strength through espionage, disruption and theft. Attempts to obtain IP data on vaccines and attacks against software supply chains demonstrate the lengths to which nation states are prepared to go to achieve their strategic goals.*
>
> –Dr. Mike McGuire,
> Senior Lecturer in Criminology at the University of Surrey

STRENGTHEN CYBER DEFENSES WITH NEXSAN'S UNBREAKABLE BACKUP

Without a secure backup copy, organizations risk total loss of their data and their operations following a successful cyberattack. Nexsan's Unbreakable Backup solution safeguards all your unstructured data - all the way through your backups.

In the fight against cyberattacks like ransomware and other forms of malware, Unbreakable Backup makes recovery of unaltered files fast and easy so there's no disruption. Thanks to the advanced technology of Unity and Assureon, an active data vault, the solution works together to create an immutable copy of any data to ensure data recoverability.

Contact us today if you are ready to learn how Unbreakable Backup can strengthen your data security.

Nexsan | 1289 Anvilwood Ave, Sunnyvale, CA 94089 | sales@nexsan.com