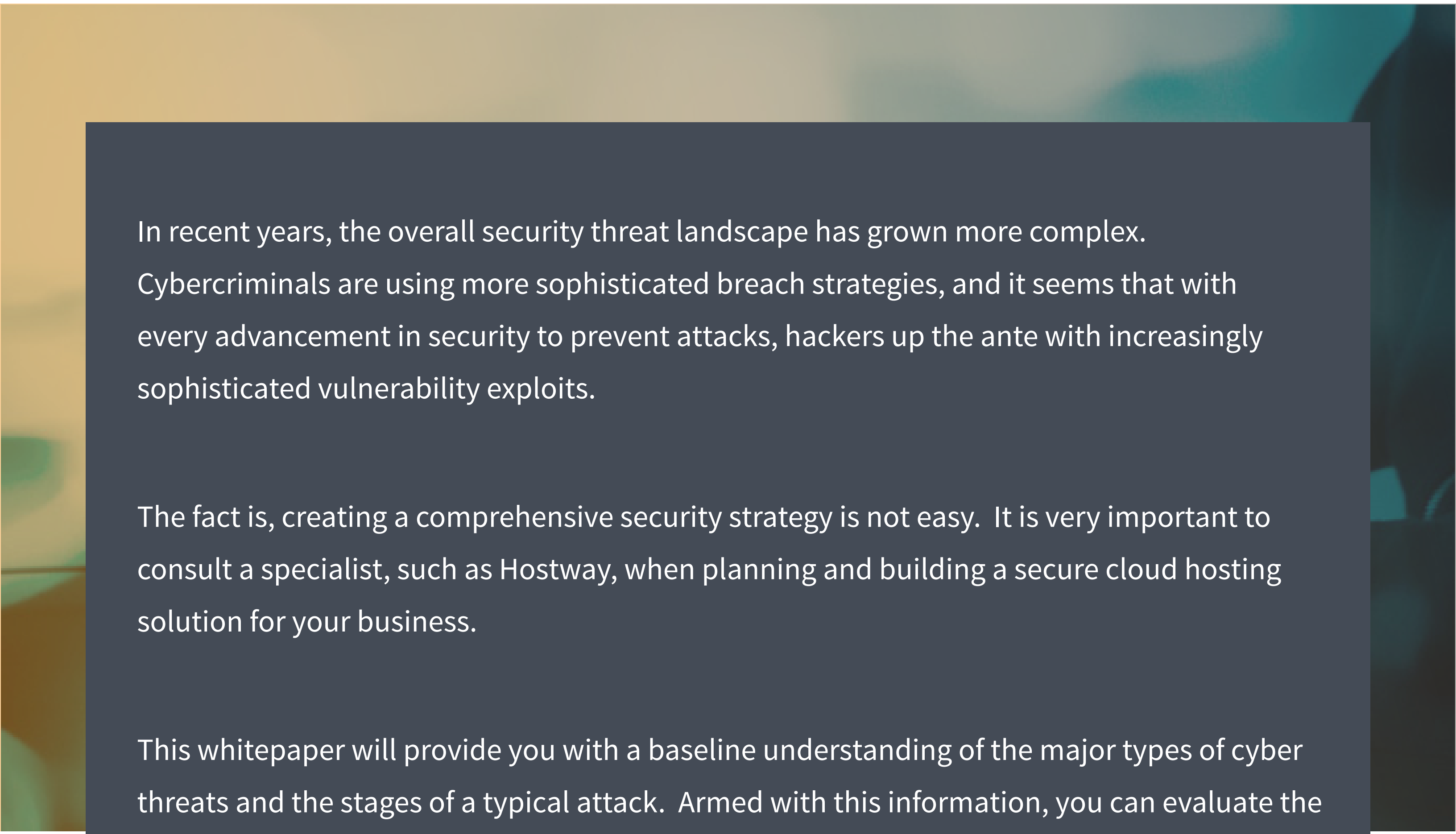
HOSTWAY®
THE TRUSTED CLOUD

The 6 Stages of a Malicious Cyber Attack

Is Your Business Secure?



In recent years, the overall security threat landscape has grown more complex. Cybercriminals are using more sophisticated breach strategies, and it seems that with every advancement in security to prevent attacks, hackers up the ante with increasingly sophisticated vulnerability exploits.

The fact is, creating a comprehensive security strategy is not easy. It is very important to consult a specialist, such as Hostway, when planning and building a secure cloud hosting solution for your business.

This whitepaper will provide you with a baseline understanding of the major types of cyber threats and the stages of a typical attack. Armed with this information, you can evaluate the risk for your business and construct the appropriate security strategy.

Today's Top Threats

When one thinks of a breach, an image of a shadowy hacker crouched behind a laptop usually comes to mind. This individual is typically motivated by financial gain, seeking to steal data that can then be sold on underground marketplaces or used for fraudulent activity.

The two most prominent types of external threats include efforts to compromise web applications and distributed denial-of-service (DDos) attacks.

- **Web Application Compromise:** According to the 2016 Verizon Data Breach Investigations Report, the majority of confirmed breaches result from attacks aimed at web applications. These compromises are often seen in the finance, entertainment, and education industries, and enable hackers to leverage an organization's own online platform against itself.

Vulnerabilities like injection strategies, weak authentication credentials, and improper session management, as well as the misconfiguration of security measures can enable a cybercriminal to compromise a web app.

- **Distributed Denial-of-Service (DDos) Attacks:** DDoS attacks have become more prevalent across nearly every industry, aside from health care. In fact, 2016 saw the largest DDoS attack to ever take place to date. The event centered on servers managed by internet performance management firm Dyn, and affected access to websites including Twitter, Netflix, CNN, and Reddit. An investigation showed that as many as 100,000 malicious endpoints were used to support the 1.2 Tbps attack, overwhelming Dynservers until they collapsed under the inundation of traffic.

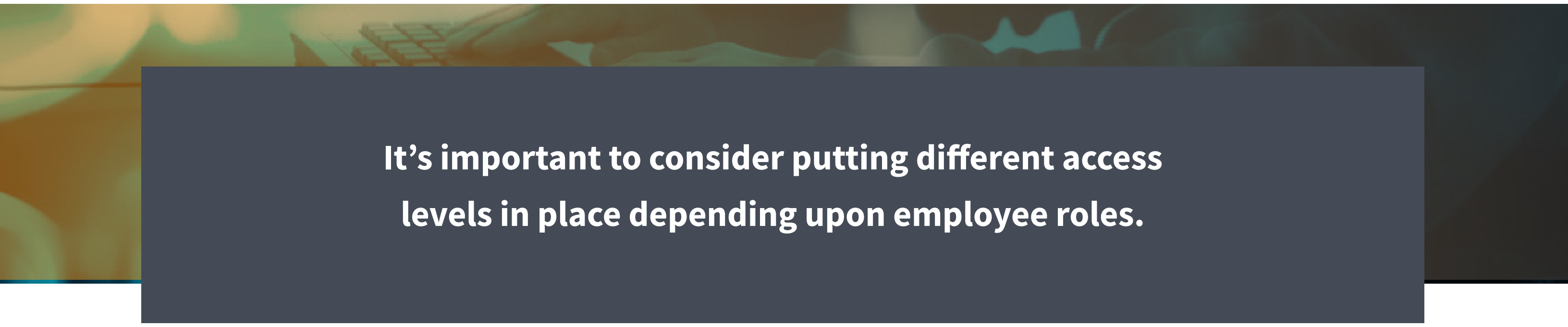
Stages of a Breach: How Malicious Attacks Take Place

Risks can emerge from a variety of avenues. However, when an attack does take place, it typically follows a standard set of stages:

1. Reconnaissance: First, malicious actors seek to learn as much about the target as possible. Knowledge of the victim organization's infrastructure and security measures are used to inform the attack strategy.

2. Scan: Next, a hacker will scan the system for vulnerabilities that can be leveraged to launch the attack. This can include seeking out open ports, older or unpatched systems, or versions of technology with known exploitable risks.

3. Exploit: Once a vulnerability is discovered, the attacker uses this to begin the attack. In some cases, the first attempt at exploitation is successful and the hacker moves onto the next stage. Other instances see the use of multiple exploits to break through different systems within company infrastructure as the attacker looks to target a specific platform. For instance, a cybercriminal may attack an organization's website, and use it as a launch pad to exploit a connected system containing much more valuable data.



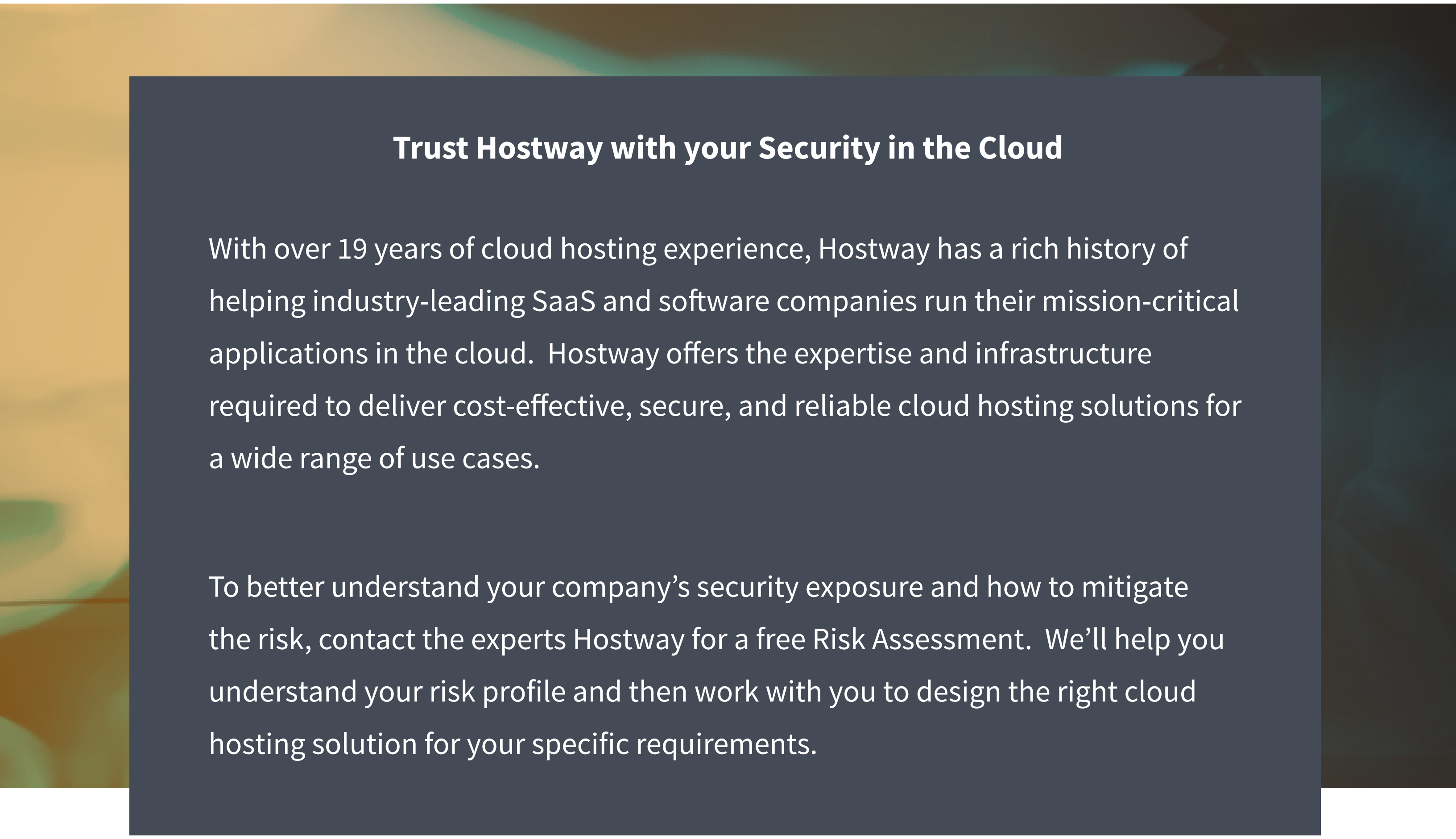
It's important to consider putting different access levels in place depending upon employee roles.

4. Maintain Access: Once inside the system, a hacker will look to maintain a presence there for as long as he can. This allows him to gather as much data as possible. Many attackers will also put a backdoor in place that's invisible to the organization, but provides the cybercriminal with a simple way to attack again at a later time.

5. Exfiltration: This stage sees the actual theft of the victim's data. After gathering as much valuable information as possible - including everything from client details to proprietary company data - the attacker will transmit it to a protected server under his own control.

6. Prevent Identification: Finally, the cybercriminal will work to disguise any clues of his malicious presence. This process can include altering activity logs, changing files and doing everything possible to block the organization from realizing that an attack has taken place.

With a solid understanding of the threat landscape and strategies hackers use to compromise and exploit IT systems, organizations can proactively take steps to prevent a breach of sensitive data (see Hostway whitepaper – 6 Best Practices for Preventing a Security Breach).



Trust Hostway with your Security in the Cloud

With over 19 years of cloud hosting experience, Hostway has a rich history of helping industry-leading SaaS and software companies run their mission-critical applications in the cloud. Hostway offers the expertise and infrastructure required to deliver cost-effective, secure, and reliable cloud hosting solutions for a wide range of use cases.

To better understand your company's security exposure and how to mitigate the risk, contact the experts Hostway for a free Risk Assessment. We'll help you understand your risk profile and then work with you to design the right cloud hosting solution for your specific requirements.

HOSTWAY®

THE TRUSTED CLOUD