Threat Actors

Instructor: Data breaches can expose sensitive personal information such as Social Security Numbers, birthdates, and financial account data. This information can be used by criminals for fraud and identity theft. Billions of records have been stolen through data breaches in recent years. A breach can cause a company to suffer fines and penalties while eroding shareholder value, brand trust and consumer confidence.

Annual reports like The Verizon Data Breach Investigations Report analyze security incidents including data breaches. They report attacks commonly occur through point-of-sale methods, web applications, physical theft, malware, denial of service, and miscellaneous errors. Hacking continues to be a common attack. Cybercriminals exploit vulnerabilities like misconfigured services, unpatched systems, and naove humans through social engineering, to achieve unauthorized access to data.

While the term hacker is many times associated with a cybercriminal, hacker is a broad category for a wide swath of actors with varying intentions. For instance, there are ethical hackers are who authorized to attempt a system breach for vulnerability testing. White hats, red teams and blue teams are examples of an ethical hacker.

But there are several types of hackers with a range of criminal motives:

Black hats and script kiddies typically seek targets out of revenge or opportunity. Some of the more dangerous hacker types are involved in espionage, or seek to create fear and mayhem, on a larger, more impactful scale, like: Hacktivists, driven by a deep conviction of beliefs, state-sponsored actors operating on behalf of a government or agency, cyber mercenaries that hack for hire, terrorists and organized mafia-type groups also have a criminal presence in cyberspace.

While a threat actor could be a cybercriminal - the external "bad guy" who launches a phishing campaign - it could also be an insider - the negligent employee who carelessly discards sensitive documents.

The latter, someone who is close to the entity, is one of the most threatening actor types if they have vengeful intent. The insider threat may be malicious insiders who are disgruntled with their employer or have been compromised by a competitor. Depending on the level of access the insider has, the vulnerability can range from physical access to unauthorized sharing of proprietary data.

Another actor type is the Advanced Persistent Threat. APTs are a funded and focused group of

attackers frequently associated with nation states or criminal organizations that have espionage, financial or political objectives. An APT attack begins with in-depth reconnaissance and network enumeration; this background research is used to identify attack targets and weak links.

Threat actors' success is typically dependent upon human nature, a misconfigured or unpatched system, or the unwitting cooperation of a victim. Phishing is one of the most successful attack types. It is a social engineering ploy that convinces a user to click a link in an email, or a stealthily placed link on a webpage that then prompts the installation of a backdoor or command-and-control malware. Once an attacker has gained entry to a system they can attempt to expand their foothold, propagate malicious code, or retrieve desired information before their presence is detected.

A full defense-in-depth strategy is prudent to protect and defend against threat actors. This includes: use of multi-factor authentication patch management strategy for infrastructure to minimize exploitable software vulnerabilities. Host-based anti-virus and anti-malware controls. Access control lists and encryption properly applied to internal file servers. Intrusion and anomaly detection systems that include automated log collection, analysis,

and alerting. Spam and phishing email protections. Comprehensive user training on information security best practices, acceptable use policies, and common threat awareness. A full business risk assessment.

The last two are arguably most crucial. The risk management assessment takes a granular look at every component of the entity and identifies assets most critical to business functions, specific threats to those assets, and the most effective way to mitigate or manage those risks.

Users are the weakest link to security, so they must be aware of threats and the best practices to avoid them as well as participate in training to understand their role in the organization's security. The most stringent controls and procedures can be in place, but a single hasty action from a user can negate those security measures. Virus software can have the latest signatures applied, but a small change to malware code could enable that code to fly under the radar. It's a tough battle to stay ahead of.

Threats to information security are concerning, and threat actors are highly motivated. Prevention and defense mechanisms can be customized if an entity knows the type of attacks it may be vulnerable to and the motivations of its adversaries.

Technology has become ubiquitous in business services and functions. Consumers trust that their personal information is protected while processed, transmitted, or stored. Threat actors have a strong desire to obtain that information, and they employ many strategies to poke at entity components to find a weak entry point. Organizations have to remain a step ahead with prevention and defense best practices to avoid becoming victim to intrusion or data breach.

Notices