Three goals to protect against APTs

Cyber insurance isn't the sole answer to managing a cyber incident. At DUAL, we strongly believe that prevention is better than cure, which is why we are working with Secureworks on suggestions in protecting your organisation from threats! There are many types of threat actors that may try to get in to your system; advanced persistent threats (APTs) are just one of them.

APT is the commonly used name for sophisticated cyber espionage campaigns orchestrated by governments or their intelligence agencies. They typically involve meticulously planned and prolonged attacks aimed at infiltrating target networks, stealing sensitive information and maintaining undetected access for extended periods, leveraging a variety of tactics such as spear-phishing, malware deployment and exploiting vulnerabilities to achieve their objectives.

Secureworks recommends keeping these three goals in mind to protect your organisation against these types of threats. This advice equips you with valuable tools, but the ultimate responsibility for your online safety lies with you. Stay informed about emerging threats, and don't be afraid to seek additional guidance from trusted sources if something seems suspicious. At DUAL, we encourage organisations to be proactive with their incident response plan, which lays out the guidelines for responding to a cyber incident. One key workstream is the legal and regulatory implications.

Goal #1

Make it hard for threat actors to get inside your network.

Patching

Patch all systems, especially internet-facing servers, firewalls, VPN and remote access gateways, and Citrix portals. Prioritise vulnerabilities mentioned in cisa.gov/known-exploited-vulnerabilities-catalog

MFA

Ensure MFA is implemented using the latest phishing-resistant technology (tokens, authenticated devices) and mandated for all remote access.

Anti-malware

Ensure complete coverage of good endpoint protection tools (Next-Gen Antivirus software).

Cloud

Secure your cloud configuration leveraging cloud provider tools and experts who can help you reduce your cloud attack surface.

Testing

Conduct external pen testing/red teaming often to ensure any ways in are identified and remediated before they are exploited.

Employees

Nurture employee loyalty and train employees in good security practices.

Goal #2

Make it hard for threat actors to remain undetected once they're in.

Harden

Harden default system configuration on all internal resources.

Active directory

Harden active directory to prevent privilege escalation and mass deployment of malware.

Visibility

Ensure you have full XDR visibility (endpoints + network devices + cloud + applications) and 24/7 threat monitoring by a competent security operations team.

Honeypots

Use honeypots and honey tokens as an early warning system.

Threat hunt

Leverage threat hunting techniques to detect the presence of threat actors in your network.

Goal #3

Conserve energy. When you move, strike hard.

Threat intelligence

Invest in good threat intelligence to help understand what tactics you may be faced with.

IR planning and exercising

Plan the response that you will take when threat actors strike.

Calculate

Keep a cool head when faced with the adversary. Hire experts in dealing with APTs to help (a CIR Level 1 provider from ncsc.gov.uk/schemes/cyber-incident-response/find-a-provider).

Helping you do more

One Creechurch Place, London EC3A 5AF

dualinsurance.com

DUAL | Secureworks®