Kaspersky for Business

KASPERSKY lab

$100,000

Average cost of an undetected threat to your business

What is an APT?

APT stands for "Advanced Persistent Threat." APTs are "advanced" because the tools used in these attacks are more sophisticated that those usually used by cybercriminals. They are "persistent" because once and organization is breached, the malware can remain in the system for months or even years. APTs are usually targeted attacks and make up 1% of the threat landscape, using techniques such as spear phishing, exploits and rootkits or bootkits to conceal their presence.

What is a zero day exploit?

A zero-day vulnerability is an undisclosed computer-software vulnerability that hackers can exploit in order to adversely affect computer programs, data, additional computers or a network.

APTs by the Numbers

21% Had incidents affecting suppliers that we share data with.*

22% Lost access to customer-facing services as a result of a targeted attack.*

25% Companies who say they have definitely experienced an APT attack.**

34% Companies who experienced damage to their company's reputation as a result of an APT attack.**

68% Experienced a targeted attack on their networks and suffered data loss as a direct result.*

78% Companies who experienced downtime as a result of an APT attack.**

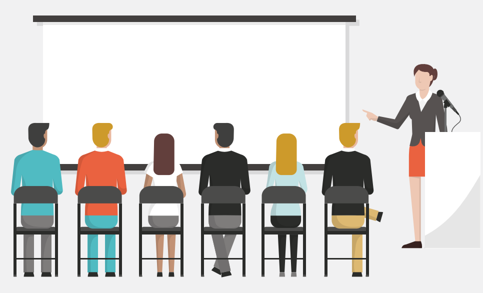
*_Corporate IT Security Risks Survey 2016_ from Kaspersky Lab and B2B International

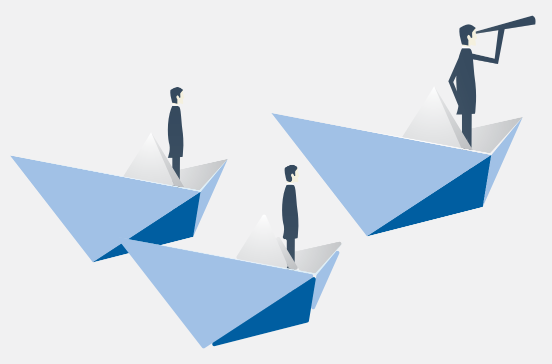
**IDG Marketpulse 2017 Survey on "Advanced Persistent Threats"

How do you protect yourself from APTs?

1 **Your employees are your first line of defense.** Because many APTs gain access to an organization via spear phishing emails or social engineering, you should make sure that employees know and observe company policies.

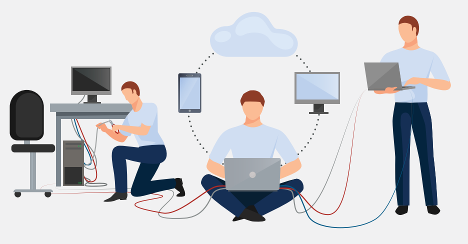
2 **Employee education sessions are well worth your time.** 80% of cybersecurity incidents start with a human mistake. Training works, especially when you use varied and creative methods that hold people's attention and reinforce the message regularly.





3 **Your company's leaders need to promote cybersecurity awareness and devote resources towards it.** Educating employees starts at the top. When your company's leaders understand the complexities of the threat landscape, they can help your IT department promote awareness and education around the topic. And since many boards now understand that they can be held legally responsible in the event of a breach, many are more eager to support such programs.

4 **Communication is key.** All employees should know how to inform IT in the event of a breach or any suspicious activity.

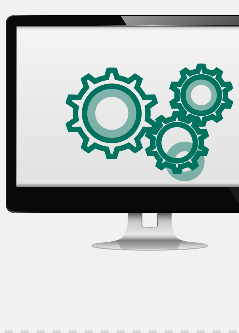


5 **Maintain control over user access rights and privileges.** Know who needs access to which programs, devices and sensitive information.

6 **Record all rights and privileges.** When you have a security incident, knowing who has access to which part of your organization can save you a lot of time.

7 **Perform regular scans in order to catch system vulnerabilities and keep your network services up to date.** Because systems and networks are constantly changing, it's important to scan them for vulnerabilities regularly.

8 **Update policies and procedures as necessary.** When you preform regular scans, you will catch certain vulnerabilities and learn new information about your network. It's important to assess whether or not you need to update new policies and procedures.



9 **Update vulnerable components and applications.** Patch management is essential. Do it regularly.

10 **Install a multi-layered security solution.** None of the above matters if you do not have a robust, multi-layered security solution installed on your system that can catch the vulnerabilities that are inevitable with human error.

For more on APTs, download our eBook, _Whodunit: The Mystery of the APT_.

To learn more about KATA (Kaspersky Anti-Targeted Attack) platform, download our data sheet.