ISRAELDEFENSE

Day Tuesday, כ' תמוז התשע"ח
03.07.2018

Cyberattack – an Act of Terror

The battle against cybercrime is very similar to the fight against terror. The amount of threats, their complexity, and their damaging potential require a prompt, dynamic, and proactive approach. Consequently, organizations should adopt counterterrorism strategies and tactics to protect themselves effectively on the cyber battlefield

Sharon Nimirovski | 3/07/2018

Send to printer | Send to a friend | Size | Share on | Share on

Illustration: Bigstock

In 2016, the global cybercrime industry was worth around $500 billion, a staggering figure as far as global market size is concerned. In comparison, the illegal drug trade was worth around $350 million in 2016. However, while involvement in the drug trade poses a significant risk, the average hacker operates out of his home, or from a coffee shop, using his laptop computer – a perfect disguise with almost zero risk.

We currently witness more cyberattacks targeting organizations and evolving all the time. In order to make money through cybercrime, one does not have to be a hacker. A possible definition for this controversial pursuit is “Crime as a Service.” Using the Internet, one can easily acquire a “crime bundle,” some of which are even available free of charge, and start attacking any target, without understanding how the bundle works, and earning money immediately. With these simple-to-use applications, combined with the opportunity to make easy money, it is no wonder that thousands of cyberattacks occur every day. Hackers can trade the information they draw from their targets for money – at practically no risks to themselves.

The world's IT security industry and cybersphere generally invest thousands of working hours and hundreds of thousands of dollars annually in upgrading the tools and knowledge for defending against these attacks, mostly in the public and business sectors. In Israel, the National Cyber Security Authority (NCSA) monitors privately initiated attacks, among others. On the other hand, experience has shown that such leading information security companies like Check Point, Palo Alto, Kaspersky and others can respond to threats only after 48 to 72 hours. In the cyber world, this is a very long time. The reason for that stems from the difficulty of identifying cyberattacks where the attack models change their patterns every day. In addition, the security companies tend to respond “across the board” rather than focus on the specific organization facing the attack.

Having said that, the defense protocols used by most organizations evidently fail to provide a proper response for cyberattacks, especially in the era of business agility and broad perspectives. Consequently, almost every ransomware tool can easily bypass all familiar defense layers. The amount of threats, their complexity, and their damaging potential compel organizations wishing to protect themselves to adopt a prompt, dynamic and proactive approach. If they fail to protect themselves, their investments in resources (equipment and personnel) will go down the drain repeatedly.

Every cyber threat needs to be spotted while the spotting party remains as effectively protected as possible. In Israel, military cybersecurity elements gained substantial experience over the years, from which one can derive and implement methods of operation. The Israeli military teaches its cybersecurity specialists to “sleep with the enemy” – to know the enemy, think like the enemy and act like the enemy. This military strategy is the most appropriate one for dealing with cybercrime – we need to completely forget that we are on the defensive side and start thinking about what our most painful spot would be, what our weakness is, where the damage potential is the most substantial – and focus on those spots. We must remember that yesterday's methods are not necessarily relevant today.

The recognition of the effectiveness of this approach has permeated even more deeply this year, along with the realization that a cyber war is an all-out war on terrorism. Israel is perceived as a global innovator in the field and as a leading exporter of defensive cybersecurity software, converted from military applications. In practice, however, the Israeli Government does not promote sufficient regulation in this field, and various local companies that are not legally obligated to comply with even the minimum information security criteria endanger multiple parties.

Just recently, we have learned that the Israel Capital Market, Insurance & Savings Authority found cybersecurity faults at various institutional entities – insurance companies, pension funds, provident funds, and education funds – in which the public invests billions of shekels. The Authority is currently conducting a comprehensive audit of this industry, to determine how to manage the cybersecurity risks it faces. One can only hope that in the race against time in cyberspace, these faults are addressed in accordance with the military concept, in order to gain even a small advantage on the cyber battlefield.

***

Sharon Nimirovski is the CEO of White Hat

Send to printer | Send to a friend | Size | Share on | Share on

Boeing Invests in On-Demand Urban Aerial Delivery Startup Matternet ❯

IDAN Computers Presents ObliMapper – Transforms Drone Imagery into Actionable VISINT ❯

Cyberbit Hosted Joint Cybersecurity Exercise for German, Israeli Banks ❯

You might be interested also

Thai Army Operates Elbit Hermes 450 UAVs

Ami Rojkes Dombe | 26/06/2018

[Reports: Israeli Missiles Strike Arms Depots near Damascus Airport](#) ❯

http://thaidefense-news.blogspot.com/2018/05/royal-thai-army-uav-21st-av...