Why we should all care about cyber crime

August 5 2015, by Mihai Lazarescu

No one is immune from cyber crime… no matter how protected you think you are. Credit: Flickr/Louish Pixel, CC BY-ND

In today's world, the reality is that all individuals and organisations connected to the internet are vulnerable to cyber attack. The number, type and sophistication of attacks continues to grow, as the threat report published last month by the Australian Cyber Security Centre (ACSC) points out.

It isn't only large organisations that are under threat. Even individuals or organisations that don't believe they have much to offer hackers can be

targeted. So even if you think you're a small target, you might still be at risk.

Illusion of trust

Malicious individuals and groups thrive on gathering information that can be used to enhance their attack strategies. Hackers are becoming more focused on spear-phishing attacks, which are tailored to individual people, and any bit of information about you can be of help.

Key to the hacker is the issue of trust. The information gathered is used to build a profile of the target with the aim to have enough data that allows the hacker to appear trustworthy to you.

In most cases, the hacker will attempt to impersonate an entity that is trusted by you. The more information the hacker has on you, the more likely they will be able to maintain the illusion long enough to achieve their aims.

The effects of a successful attack vary significantly, largely depending on the motivation of the hacker.

For most of us, identity theft is likely to cause the most damage because it badly impacts on our ability to go about our normal daily life. Our credit rating could be severely compromised, for example. To make matters worse, the process of addressing the damage of an attack can be costly, time consuming and emotionally exhausting.

In other cases, the damage could be in the form of confidential information, such as medical history records, ending up in the hands of malicious parties, and thus make the you susceptible to different kinds of blackmail.

The recent breach of the Ashley Madison website is a typical example of confidential information about individuals that could be exploited by malicious parties.

Your access is important to hackers

But specific personal information is not the only driving factor behind cyber attacks. Often, the resources or the access you have to other systems is the overall goal.

A common misconception held by many individuals and organisations is that if they do not have anything of value on their systems, they are not likely to be attacked. Or the hackers have nothing to gain from copying all their information.

The information value may be zero, but the resources are precious commodities which can be easily used in two ways:

- to launch more intensive, distributed attacks on the hacker's primary target
- they can be "leased out" in the form of botnets to other parties.

From the point of the user clearance, hackers again can exploit the knowledge about the target to attempt to gain access to difficult to reach systems.

Food for hacking thought

I was told of one case in the US where foreign hackers used the eating habits of the staff of a government organisation (obtained from credit charges) to launch a "watering hole" attack.

The hackers were able to easily compromise the server hosting the website of the restaurant frequented by the government employees and replaced the original PDF menus with a new set that had malware embedded in them. Thus, when the government employees were viewing the menus from their secure machines, they were downloading the malware as well.

These are just some of the ways hackers can take advantage of the information gathered from attacks. Unfortunately, the only limiting factor is the creativity of the malicious party. And sadly, hackers are very creative.

Beating cyber attacks

The attitude of individuals and organisations needs to change in order to prevent cyber attacks. There has to be a fundamental understanding that, when online, everyone is a target and that none of us are too small or unimportant.

It is also critical to change the attitude to incident detection and handling. We can only get better at the defence part if we learn from previous experience, painful and costly as that may be. The reason we know about some of the attacks mentioned above is because they were detected and investigated.

Most organisations do not consider incident handling as a core component of cyber defence. And as long as that continues, the improvement in the cyber defences will be slow.

There has to be a concerted effort to treat cyber security seriously rather than an expensive auditing exercise. The vast majority of organisations are looking at cyber security as a compliance task and thus do the minimum possible to achieve that.

The payment card industry's Data Security Standards for major credit cards is a classic example. It is good that there is a standard, but what is unfortunate is that all organisations try to do is the absolute minimum possible to pass the standard check rather than actually improving their security.

Instead the view should be to use the cyber security requirements as a way to improve overall security and thus avoid costly and damaging incidents in the future.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation