CANADIAN CENTRE FOR CYBER SECURITY RELEASES RANSOMWARE PLAYBOOK

Posted on December 21, 2021

Categories: Insights, Publications

Ransomware attacks are on the rise.

In the first half of 2021, global ransomware attacks increased by a staggering 151%.[1] Throughout the year, the world has seen many high profile ransomware attacks on large organizations, including the widely publicised attacks on Kaseya and Colonial Pipeline.

The Canadian Centre for Cyber Security ("**CCCS**") has proposed several reasons for the increase in ransomware activity, including the shift towards online operations throughout the pandemic and the increasing sophistication of cybercriminals.[2] Perhaps most troubling is the emergence of "ransomware-as-a-service", in which developers sell or lease their ransomware programs to other cybercriminals, taking a percentage of the victim's ransom payment in return.[3]

Nonetheless, as the CCCS has noted, organizations can prevent or mitigate the vast majority of ransomware attacks by implementing basic cyber security measures. This is why on November 30, 2021, the CCCS released a ransomware playbook (the "**Playbook**") to help organizations prepare for and respond to ransomware attacks.[4]

What is Ransomware?

Ransomware is a type of malicious software that threatens to publish a victim's data assets or perpetually block access unless a sum of money is paid. Ransomware incidents can devastate organizations by disrupting their critical functions reliant on network and system connectivity.

What Companies Do Cybercriminals Target?

Businesses of all sizes can be targets of ransomware attacks. While attacks on larger corporations can be more lucrative for cybercriminals, as the Playbook notes, cybercriminals often consider small and medium sized organizations to have weaker security protection measures, making them easier targets.[5]

The following factors make a company a more likely target for a ransomware attack:

- The company has access to sensitive data that can be directly exploited, such as social insurance numbers, credit card numbers, or other financial information;
- The company has access to personal information that individuals would not want to be exposed, such as medical or religious information;
- Data is a crucial component of the company's business, such that a disruption to the company's systems would halt their entire business (making the company more likely to pay the ransom);
- The company holds valuable client data, or intellectual property, such as trade secrets;
- The company takes part in critical infrastructure, such as vital medical services; or
- The company is connected to a company that meets one of the descriptions above.[6]

The first half of the Playbook focusses on how a company can defend against ransomware. It covers cyber defence planning and basic cybersecurity controls. On the subject of cyber defence planning, the Playbook provides a useful overview of the principles to consider when developing (i) a backup plan, (ii) an incident response plan, and (iii) a recovery plan.[7]

In terms of cybersecurity controls, the Playbook provides a list of useful data security measures, including, without limitation:

- **Perimeter defences**, such as firewalls, anti-phishing software, and virtual private networks;
- **Logging and alerting**, to track activity throughout the system, which helps establish an audit trail;
- **Penetration testing**, to assess vulnerabilities;
- **Network Segmentation**, to control and restrict access to information within your IT system; and
- **Password management**, to ensure stronger passwords are used throughout your organization.[8]

The second half of the Playbook focusses on how to recover from ransomware attacks. It covers immediate response actions that companies should take in the event of a breach and actions that will help a company get their business back online as quickly as possible following an attack.[9]

The Playbook is a useful tool for companies of all sizes to assess their readiness for a ransomware attack, and prepare themselves accordingly. However, companies need to employ a contextual approach to data security, taking into account the nature of their business, as well as their data and security systems. Developing and maintaining a comprehensive ransomware strategy requires input from legal and IT professionals.

If you have experienced a ransomware attack, or you have any questions about how to prepare for potential ransomware attacks, a member of our privacy and data security group would be happy to assist you.

[1] As compared with the latter half of 2020: Canadian Centre for Cyber Security, *Cyber Threat Bulletin: The Ransomware Threat in 2021*.

[2] Canadian Centre for *Cyber Security, Cyber Threat Bulletin: The Ransomware Threat in 2021*, s.v. "Evolving Trends".
[3] Canadian Centre for Cyber Security, Cyber Threat Bulletin: The Ransomware Threat in 2021, s.v. "Ransomware-as-a-Service".
[4] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099.
[5] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099 at 1.1.2.
[6] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099 at 1.1.2.
[7] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099 at 2.1.
[8] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099 at 2.2.
[9] Canadian Centre for Cyber Security, Ransomware playbook ITSM.00.099 at 3.

by Mitch Koczerginski and Robbie Grant

A Cautionary Note

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.