Guidance For Defending And Responding To Ransomware Attacks

November 25, 2016

Ransomware attacks are a significant and increasing threat to organizations of all kinds. The U.S. Federal Trade Commission recently issued guidance regarding ransomware attacks. Organizations should consider that guidance and take appropriate steps to defend against, and prepare to respond to, ransomware attacks.

Ransomware

Ransomware is malicious software that prevents access to or use of an infected information technology device or system (an "IT Resource") or related data, and demands (typically through an on-screen warning or other form of ransom note) that a ransom be paid (often in virtual currency or other forms of untraceable payment) to obtain a key to restore the infected IT Resource or data. There are two basic kinds of ransomware: “locker” ransomware (which prevents use of an IT Resource by locking the user interface) and "crypto" ransomware (which encrypts specific files or data so they cannot be used without the required decryption key).

Ransomware is often installed on an IT Resource through fraudulent techniques, such as a deceptive email with a malicious attachment or link (known as "phishing" or "spear-phishing"), surreptitious downloading from an infected website (known as "drive-by downloading") or an infected message on a social media site. Sophisticated ransomware can spread throughout a computer network (including to data stored in cloud services) before the ransomware activates, and can install other kinds of malware.

While many hackers profit by stealing data, ransomware criminals profit by demanding ransom payments from organizations and individuals whose IT Resources and data are affected by the ransomware. The primary result of a ransomware attack is business disruption and loss of use of data to the victim organization, rather than harm resulting from unauthorized disclosure of data. Nevertheless some ransomware attacks can also result in hackers obtaining access to data.

A ransomware attack can cause significant financial loss and other harm to the victim

organization, including: (1) temporary or permanent loss of use of IT Resources and data; (2) business disruption loss and resulting liability to customers and business partners; (3) costs to restore infected IT Resources and data, if possible, and to otherwise respond to the ransomware attack; and (4) harm to the organization's reputation and relations with customers and business partners. Ransomware can also cause significant financial loss and other harm to the victim organization's customers and business partners who depend on the organization's products and services.

Paying a ransom is risky because the payment encourages ransomware criminals and does not guarantee that required restoration codes will be provided or that other undisclosed malware will be removed from the infected IT Resource. In some instances, a ransomware criminal will increase the ransom demand if the victim indicates a willingness to pay. Nevertheless, ransomware victims often chose to accept those risks and pay the ransom to avoid the cost, delay and other adverse consequences of relying on alternative remedies (e.g. attempting to restore infected IT Resources and data) if any are available. For those reasons, the number and sophistication of ransomware attacks have increased over recent years and are predicted to continue to do so.

Federal Trade Commission Guidance

On November 10, 2016, the United States Federal Trade Commission ("FTC") issued basic ransomware guidance (How to defend against ransomware and Ransomware – A closer look) and an accompanying video (Defend against Ransomware) to help consumers and businesses defend against and prepare to respond to ransomware attacks. The guidance for defending against ransomware includes:

- **Awareness:** Educate and train personnel to exercise caution online and avoid phishing emails that deliver ransomware.
- **Cyber Hygiene:** Identify security risks and implement appropriate technological measures to protect against ransomware, including network security and email hygiene products, intrusion prevention (anti-malware) software and timely installation of security updates for all software (operating systems, security software, web browsers and applications).
- **Data Backups:** Regularly back up important data from all computer systems and devices, and safely store the backups on devices that are not connected to a network.
- **Plan:** Develop and test incident response and business continuity plans for responding to ransomware and mitigating resulting business disruption.

The guidance for responding to ransomware includes:

- **Containment:** Quickly contain the ransomware (e.g. disconnect infected devices from the network) to prevent the ransomware from spreading to other devices and the network.
- **Implement Plans:** Implement incident response plans and business continuity plans, and use reliable backups to restore data and systems to uninfected or properly cleansed devices.

- **Contact Law Enforcement:** Report the ransomware attack to law enforcement. The FTC's guidance cautions against paying a ransom, but acknowledges that a ransom payment might be necessary in some circumstances.

The FTC's guidance is consistent with other guidance from Canadian and United States regulators, including Alerts issued in March and April 2016 by the Canadian Cyber Incident Response Centre and the United States Department of Homeland Security Computer Emergency Readiness Team, Advisory for Ransomware issued in March 2016 by the Alberta Privacy Commissioner and Protecting Against Ransomware Technology Fact Sheet issued in July 2016 by the Information and Privacy Commissioner of Ontario. For more information, see *Government Guidance for Preventing and Responding to Ransomware Attacks*.

Comment

An organization should prepare to respond to a ransomware attack by establishing and testing a detailed incident response plan that will enable the organization to make important technical, business and legal decisions in a timely manner. Those legal decisions may include whether the organization should give notice of the ransomware attack to regulators (e.g. privacy commissioners), affected individuals (e.g. customers), other organizations (e.g. business partners), stakeholders (e.g. shareholders and investors) and insurers. In many circumstances, an organization might have a legal obligation (under statute, generally applicable common or civil law or contract) to give notice of a ransomware attack. In addition, there might be important business reasons to give notice of a ransomware attack even if there is no legal obligation to do so. Organizations should obtain appropriate technical and legal advice when preparing a cyber incident response plan and when responding to a ransomware attack.

By

Bradley Freedman

Expertise

Cybersecurity, Privacy & Data Protection

BLG | Canada's Law Firm

As the largest, truly full-service Canadian law firm, Borden Ladner Gervais LLP (BLG) delivers practical legal advice for domestic and international clients across more practices and industries than any Canadian firm. With over 725 lawyers, intellectual property agents and other professionals, BLG serves the legal needs of businesses and institutions across Canada and beyond – from M&A and capital markets, to disputes, financing, and trademark & patent registration.

blg.com

BLG Offices

Calgary

Centennial Place, East Tower
520 3rd Avenue S.W.
Calgary, AB, Canada
T2P 0R3

T 403.232.9500
F 403.266.1395

Ottawa

World Exchange Plaza
100 Queen Street
Ottawa, ON, Canada
K1P 1J9

T 613.237.5160
F 613.230.8842

Vancouver

1200 Waterfront Centre
200 Burrard Street
Vancouver, BC, Canada
V7X 1T2

T 604.687.5744
F 604.687.1415

Montréal

1000 De La Gauchetière Street West
Suite 900
Montréal, QC, Canada
H3B 5H4

T 514.954.2555
F 514.879.9015

Toronto

Bay Adelaide Centre, East Tower
22 Adelaide Street West
Toronto, ON, Canada
M5H 4E3

T 416.367.6000
F 416.367.6749