Cybersecurity for Asset Managers

Protecting Your Assets

Linedata

Email, web and malware threats can put your very livelihood at stake.

Data is the lifeblood of most businesses, and nowhere is this truer than in asset management.

Where criminals once robbed banks to steal physical cash, they now know digital assets – from client data to investment strategies and algorithms – represent an instant source of untold wealth.

Identifying your (data) assets, understanding where data is stored, and securing it against attack should be a top priority to ensure this valuable information keeps making money for you and your clients – and not for cyber attackers and other bad actors.

Let's look at some of the key threats to your (data) assets, and how to protect yourself against them.

The CIS Controls Framework

To help organizations address cyber risks, the Center for Internet Security (CIS) has developed the CIS Controls™, a set of best practices informed by the field experience of senior cyber experts from a broad range of industries.

Data Breaches

Among the most infamous cyberattacks are data breaches that have cost companies hundreds of millions in fines and top CEOs their jobs, to say nothing of the business, reputational and legal damage they inflicted.

Whether securing business IP or your clients' information, there are several key steps that you should follow. These include maintaining an inventory of sensitive information and removing infrequently used sensitive information from the network. Data on mobile devices should be encrypted, and USB devices should be carefully managed, or not used at all.

> Cybersecurity accountability starts at the top. CEOs – even more than IT executives – are being blamed and punished for cybersecurity-related incidents.
>
> **Source:** Gartner

Email and Web-based Threats

A workplace without emails and web browsing is hard to imagine. Most of us use email with little thought about the cyber risks it poses. Or, we count on spam filters and browser-based controls to shield us from harm.

Such protections are far from foolproof, however. Phishing emails evade spam filters to spread viruses and ransomware and steal funds and data. Criminals use fake websites to gain access to sensitive information, including logins and passwords.

Tips for protecting yourself:

- Only use fully supported email clients and web browsers.
- Disable unauthorized email and browser plugins and add-ons.
- Use Domain Name System (DNS) filtering to block malicious web domains.
- Block email attachments if the filetypes are unnecessary for your business.
- Educate staff about phishing emails and know how to handle them.

Business email compromise (BEC) schemes – phishing attacks in which criminals impersonate executives to gain access to funds or sensitive data – have cost over

$12 Billion since 2013

Source: US Federal Bureau of Investigation (FBI)

Malware

Email is a favorite tool for spreading malware – software designed to evade or disable defenses. Malware is designed to evade or disable defenses, and threat actors constantly adapt it in order to more effectively target their victims' systems, devices and data.

To counter this threat, manage your anti-malware defenses centrally. Put in place automated scanning and rapid response processes and update all software and signatures regularly. Removable media are used to spread malware so ensure that your hardware devices automatically scan removable media (such as thumb drives) whenever these are inserted or connected.

of malware
is spread by email.

Source: 2019 Cybersecurity Almanac

Securing Your Boundaries

Strong boundary defenses have provided physical security for millennia, and border security is equally important in the digital age. You should take a layered approach, starting with knowing potential weak spots and scanning them regularly.

Keep an up-to-date inventory of boundaries and entry points, and only grant access to trusted, necessary IP addresses. Put in place monitoring systems and record network packets at each entry point. And, use vulnerability and penetration testing to identify areas of potential exploitation so these can be addressed. Remote login access to your organization's network should use data encryption and multi-factor authentication (MFA).

Heavily resourced attackers such as nation states and criminal gangs exploit weak perimeter defenses to gain footholds within organizations which they then use for further attacks.

At the same time, basic malware is available for as little as $1 at online marketplaces.

Source: Fortune

Linedata Cybersecurity Services

Want to retain expert cybersecurity support so you can focus on your business?

Linedata can help.

We offer a range of cybersecurity-related services, delivered by intelligence professionals and tailored to your requirements. By examining all security angles, we provide an ongoing view of risk, analytics and active intelligence reporting.

And, our two decades as a leading asset management solutions provider mean we truly understand your operations and security challenges – and know how to protect your assets.

Linedata

Security Risk Assessment
We review, identify and help you prioritize “at risk” areas.

Layered Defense
Full stack and layered defense strategies incorporating EDR (Endpoint Detection and Response) and threat isolation.

Vulnerability and Penetration Testing
Our threat experts identify both technical and non-technical areas of possible exploitation in your environment.

Threat Intelligence
Ongoing monitoring, alerting and actioning on new and emerging threats.

Phishing and Awareness Training
Engaging in-person or online training that educates and prepares staff for cyber events.

Policy and Controls Review
We develop and keep current regulatory compliance policies, procedures and controls.

360-degree Risk Analysis
‘Beyond DDQ’ monitoring of real-time vendor risk. Machine learning anti-virus technology plugs security holes while adapting to new traffic and providing customized alerts.

Linedata Asset Management provides a robust, configurable platform of software, data and services that enable our wealth, institutional and alternative clients to grow, operate efficiently, manage change and provide excellent service to their own clients and stakeholders.

Boston: +1 617 912 4774
New York: +1 212 607 8214
Luxembourg: +352 29 56 651
Northern Europe: +44 20 7469 8600
France: +33 1 46 11 70 00
Asia: +852 3583 7900

getinfo@linedata.com or visit: **www.linedata.com**

Linedata