ZoneFox

iGaming and the insider threat
What to spot and how to mitigate

Analyse. Detect. Respond.

The insider threat in iGaming

High cash flow, growth rate, and quantity of customers' personal data have made iGaming operations into mouth-watering targets for cyberattacks. However, pointing an accusing finger exclusively at cybercriminals somewhere "out there" would be missing the point. One of the biggest cybersecurity threats for iGaming firms, as for other sectors, is internal. People employed by an iGaming operation or who have access to the company's IT systems as a partner or provider can be the worst menace, not least because their potential for harm is often ignored until it is too late.

How can you spot insider threats?

The first step is to know how to spot situations at risk and the type of insider threat they might pose. Your company may already do such "profiling" in another context, spotting casual punters, keen gamblers, and whales by the way they bet. You can apply a similar approach to assess the chances of insider cybersecurity threats in the work environment.

Careless. PCs left unlocked and unattended. Post-Its with account passwords stuck on a screen. Downloading unauthorised software for collaboration purposes. Chatting openly about work on social networks, and clicking without checking on links in emails and websites. All these are signs of careless or unaware employees.

Disgruntled. Complaints from employees may be a sign that something is amiss. Line managers should address complaints in a timely way, whether security is an issue or not. A subtler indication of an insider attack in the offing may be a clearly unhappy employee spending more, rather than less time, at work.

Leavers. One of the most obvious risks to spot – it's simple, they're leaving! While there may be a big difference between leaving to pursue another career opportunity and being fired, both situations can lead to insider attacks.

Spies. Their efforts to blend in with their environment can make spies hard to spot. In addition, digital secrets can be stolen by copying them and leaving the originals intact. If you cannot see them before they strike, then at least you want to catch them red-handed.

Thieves. The goal of thieves is typically to sell what they have stolen to the highest bidder. You could monitor the dark web to see your data has been put up for sale, but like the spies above and at the very latest, you really want to catch thieves in the act, before they can start selling.

Prevention when you can

Prevention is better than cure – where possible. There are two main areas for action to reduce the chances of insider threats: your personnel and your IT systems.

Start by educating your personnel about proper cybersecurity. Explain that in your data-driven iGaming company, jobs depend on data being properly handled and protected. Financial loss can sink an online gaming company, but so can reputational damage after a data breach or systems attack. A

Also, make suitable checks on backgrounds and references to filter out undesirable candidates for employment. Ensure managers remain alert to defuse dissatisfaction or other workplace situations that might engender theft, espionage or sabotage, while continuing to encourage employees to handle information securely.

For your IT systems and data, apply "need-to-know" access rules. Only grant access to data or systems to those who need it to do their work correctly. This limits the potential for abuse. For example, Agatha in accounting does not need to see customer personal data in salesperson Curt's CRM system. Curt has no reason to access source code files written by Eileen in engineering either.

Likewise, have a tested, effective procedure in place when employment is being terminated. If the termination is abrupt, immediately shut down the leaver's accounts for all the assets that were available to the leaver. If there is a notice period, avoid granting new system or information access rights and for the same reason, (discretely) advise others concerned, such as the IT department, about the planned departure.

Detection when you must

Preventative measures can stop some insider threats, but not all. In that case, the priority must be on speedy, efficient, and effective detection, to contain and then eliminate attacks before they can do significant damage.

Manual or human surveillance to detect insider threats may be impractical or impossible. Instead, insider information security incidents can be better detected by automated monitoring of the information-related behaviour of users and systems. A suitable user and entity behaviour analytics (UEBA) solution can tell you if information assets are being accessed in line with normal company activity, or if there is an abnormal situation.

UEBA systems can, for example, immediately alert you to:

- Suspicious access to assets, such as an employee accessing a restricted system out of normal working hours
- Attempts to copy read-only files
- Unauthorised copying of data from a system or PC to a thumb drive
- Data being moved laterally from one system to another, possibly in preparation for exfiltration afterwards
- Connections from company systems or devices to or from unusual IP addresses.

Your immediate response will then be to investigate the situation, and stop any damage or loss as soon as possible. In the event of a cyber incident for which an employee is directly or indirectly responsible, suitable action can range from a warning and information security awareness training (for "careless", for example) to legal proceedings (for dishonest leavers) and termination of employment and legal proceedings (for thieves, spies, and possibly disgruntled, vengeful employees). In each case, a UEBA system can provide you with evidence to help you decide how to handle each case.

Conclusions

Insider threats are likely to be the greatest security risk to any iGaming organisation. To be truly effective at protecting your iGaming operation against them, your insider threat management program must include a sound understanding of the profiles linked with insider threats, and the motivations and situations that give rise to them. With this understanding and the right tools, you have a significantly better chance of mitigating these cybersecurity threats and keeping your data and IT systems safe.

To find out how ZoneFox can lock down the insider threat and secure your business-critical data, visit us at **www.zonefox.com to book a free risk assessment**, or **reach out to our security experts** and tell us how we can help.

About ZoneFox

ZoneFox helps businesses around the globe protect their business-critical data against the insider threat. Our award-winning technology provides the 360 visibility of activities around sensitive data – the who, what, where and when – by monitoring user behavior and data movement both on and off the network, and instantly alerting to anomalous activities.

Security posture is strengthened, sensitive information is protected and regulatory compliance is supported.

Like to learn more?

zonefox.com
youtube.com/zonefoxvideo
@zonefox
alerts@zonefox.com

40 Torphichen Street
Edinburgh
EH3 8JB

0845 388 4999