Electronic Gaming Risk Evaluation

OVERVIEW

WSSEA recognizes that esports is often accompanied by consumer technology suddenly thrust into a scholastic environment. The constraints of that environment may present some conflict with the technologies districts are being asked to support.

To help school districts, principals,. Directors, and IT departments evaluate when, where, and how to help esports find a home in K-12, WSSEA evaluates and shares these evaluations of gaming software titles regularly.

THE EVALUATION PROCESS

Each title is evaluated by a certified cybersecurity professional, who signs the evaluation with their name and date. The date includes an expiration, after which the evaluation by WSSEA must be renewed.

Data Categorization

WSSEA evaluates gaming titles according to how it handles data - both the operational data generated by players, as well as unique profile information that could combine to form Personally Identifiable Information.

When reviewing titles, WSSEA looks at the specific game's EULA, the game store or launcher's EULA, the gaming company's website privacy policy.

Data is evaluated based on what data is captured, where is it stored, how is it shared with third parties, and what protections the developer has in place for this data in use, in transit, and at rest.

The OSPI uses the Washington State Technology data categorizations as defined in OCIO Standard 141.10. When evaluating video gaming applications, the same standard will be applied by WSSEA.

Specifically, the categories are:

Category 1: Public data.
Public data is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

Category 2: Operational and / or sensitive data.
Sensitive data may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

Category 3: Confidential data.
Confidential data is information that is specifically protected from disclosure by law. It may include but is not limited to:

- Personal information about individuals, regardless of how that information is obtained.
- Information concerning employee personnel records.
- Information regarding IT infrastructure and security of computer and telecommunications systems.

Category 4: Confidential data requiring special handling.
Confidential data requiring special handling is information that is specifically protected from disclosure by law and for which:

- Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
- Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Note that WSSEA does not intentionally collect identifying student data, and intentionally avoids any category 3 or higher data. Category 2 data is used solely to communicate with coaches and schools.

Controls

WSSEA looks at three controls during the assessment process:

1) logical or technical
2) administrative
3) physical

Logical controls are technological, in place to protect the players and schools while using the technology itself. Software configurations to disable to adjust features, file permissions, user accounts, and firewall settings all contribute to logical controls.

Administrative controls are how players and coaches use the systems, and the people-powered processes in place to drive behavior. Having training or a policy for students to use a generic school email account when signing up for a free-to-play gaming title is an example of an administrative control.

Physical controls concern physical protection of data on hard drives by keeping gaming computers in locked rooms, under supervision, maintaining an asset inventory of equipment, and similar activities.

WSSEA evaluates available controls for schools to use that help inform a secure posture that schools and IT departments can use to work together to reduce the risk to students, schools, and our community.

A Note on Game Launchers - Client Software Footprint

PC based games are typically installed via an industry-standard Game Store (similar to the Microsoft Store). This means districts that adopt these titles for PCs on school-owned hardware will be responsible for both the gaming binaries ***and*** the game store launcher.

Each store launcher is installed in an expected directory (eg C:\Program Files\Epic Games Store\), and houses games in subdirectories. Games are installed using the permissions of the user who launched the game store.

Aside from the initial game installation, these games rarely require system-wide DLL or file registration or registry edits, meaning they are very low profile post-initial installation.

Technical controls and administrative controls work together to help manage this software, but it's worth pointing out as school districts and IT departments may find the additional requirements of a dedicated game store to be surprising.

Developer Assessments

Game developers are among the top software developers around the world. Gaming is big business, and gaming software tends to be robust and heavily tested. WSSEA evaluates four characteristics for developers:

1. Published vulnerabilities
2. Disclosure program or policies
3. Patching track record
4. Reputation in the industry

Published vulnerabilities can be found at the NIST NVD database as well as the MITRE CVE database. WSSEA checks both as part of the software evaluation process.

Developers commonly have a disclosure policy or bug bounty program. These programs are the sign of a healthy software development lifecycle that emphasizes finding and remediating vulnerabilities.
Game updates typically release a changelog, noting the patches and fixes in each release. Review of these logs indicates the game's patching history and track record of finding and fixing issues.

Lastly, using social media and news sites, WSSEA checks the developer's reputation in the game industry.

REVISION HISTORY

2022 SEP 23	Ralph Hogaboom, CISSP	Initial version