EUROPEAN FILM AWARDS
Entries Platform – Security Overview

1. Introduction

The European Film Awards Entries Platform is powered by BAFTA Nucleus.

BAFTA developed Nucleus to allow film and television makers, distributors and broadcasters to enter BAFTA's range of awards and learning programmes. The importance of the BAFTA brand as a synonym for excellence, and the damage that could be done to this through a security breach, means that security has been paramount from the very start of the project.

This goes in line with the European Film Academy's approach and therefore, the European Film Academy decided to work with BAFTA Nucleus for the film submission from 2022 onwards.

2. Network Security

2.1. Firewalls

All Nucleus instances are configured when delivered to be protected using the Amazon AWS firewall. The firewall is configured to allow public access to the web server (ports 80 and 443), but block public inbound access to all other services on the server. The only service, other than web which is available on the server is SSH (port 22). The firewall is configured so that SSH access is not public but allowed only from a limited number of BAFTA fixed IP addresses.

As an additional fail-safe, the same rules are configured on the Linux kernel firewall on the server so that even if the AWS firewall was misconfigured or accidentally switched off the same protection would be provided on the server itself.

3. Server Security

3.1. Dedicated Server

The European Film Academy as each client has its own separate instance of Nucleus running on a dedicated server. This means that even if there is a software malfunction or configuration error, there is no way that data belonging to one client can be revealed to another. This approach also means that peaks in demand for one client will not affect other clients. The size of each server can also be configured separately for each client to give the desired balance between, cost, capacity and speed.

3.2. Security Updates

BAFTA Nucleus is currently installed on Debian 10 server. This version of Ubuntu is supported until at least June 2024 and probably longer - an exact end of life date is not currently available. Each server is configured to automatically apply security updates as described here:

https://wiki.debian.org/UnattendedUpgrades

Applying updates automatically brings a very slight risk that these updates might introduce unexpected incompatibilities, but by only applying essential security upgrades this risk is minimized. We feel that the risk of allowing security vulnerabilities to go unpatched far outweighs the risk of problems from automatically applying security fixes without prior testing.

3.3. Backups

Each instance is configured to use Tarsnap (http://www.tarsnap.com/) for backups. Tarsnap is a cloud based backup service which automatically encrypts all data stored in it. Data is encrypted before it even leaves the originating machine using a 2048 bit RSA key. This means that even if the storage behind Tarsnap (which is actually Amazon's S3 service) is compromised, even then no one can read the data. This also ensures that not even Tarsnap staff can read the data of Tarsnap customers.

Each customer instance of BAFTA Nucleus is set up with a separate backup key so that one customer cannot access the backups of another customer.

4. Application Security

4.1. HTTPS

Nucleus is accessed over a secure web connection (HTTPS). The server is configured to accept unsecured HTTP connections; however it will immediately redirect the user to the equivalent secure page. Using a secure web connection means that all data exchanged between the user's browser and the server is encrypted. It also makes it impossible for anyone to set up a spoof website with the same domain name.

4.2. Password Storage

Passwords are stored in BAFTA Nucleus using the PHP password_hash function (see http://php.net/manual/en/function.password-hash.php). This is the best practice approach recommended by PHP authors. This means that even if an attacker were to gain access to the password store it would require an unfeasibly large amount of computing power to decrypt these passwords.

4.3. Brute Force Protection

A "brute force" attack consists of an attacker using automated tools to make repeated login attempts to try and guess a user's password. Nucleus automatically uses a CAPTCHA (specifically, Google's free ReCAPTCHA service) after 4 failed login attempts using the same username in any 30-minute period. This approach stops brute force attacks by requiring human input for each individual guess, whilst being completely invisible to users for most of the time. Crucially this approach avoids the administrative burden and user frustration of account locking-based approaches.

4.4. Password Strength

Nucleus provides functionality to stipulate a minimum length and maximum age for administrator passwords. This functionality currently only applies to administrators i.e. there are currently no age, complexity or length requirements for entrant account passwords.

4.5. Permissions model

Nucleus implements 2 levels of permissions for administrators. "Superusers" can see and administer all entries and all aspects of the system except for finance-related fields (see below). Ordinary administrators (non-superusers) cannot see or edit entries for the awards which have not been assigned to their user. Non-superusers cannot change which awards are assigned to them.

A third permission which can be assigned to administrators (be they superusers or not) is a finance permission. Only administrators who have been assigned the finance permission are allowed to perform sensitive operations relating to modifying pricing and invoices.

4.6. Penetration Testing

Most software authors will claim that their systems are secure, but the real proof of the pudding is when this is put to the test by independent security experts who have been tasked with finding security vulnerabilities. This is called “penetration testing”. BAFTA Nucleus has been subjected to penetration testing by security experts at Matta Consulting (http://www.trustmatta.com). This was an invaluable exercise which highlighted several potential weaknesses which we were able to fully address. We are happy to share their report and details of the actions taken in response to it with prospective customers once an NDA has been signed.

5. Notification of Security Breaches

If BAFTA or the European Film Academy become aware of any evidence of a security breach on any client instances of Nucleus, or if any security vulnerabilities are found in the Nucleus Codebase then BAFTA will inform all clients as soon as possible and at most within 48 hours of becoming aware of the problem. We will notify clients by email followed up with a phone call.

In the event of a security breach of any client instance of Nucleus, BAFTA will work with the client to take any steps necessary to secure the instance and provide any available system logs to the client for analysis. We will provide details of the nature of the breach including, the type and quantity of information that may have been affected and the measures taken or proposed to be taken to address breach. We will also provide clients with details of any relevant steps they, or their users, can take to mitigate the risks arising from the breach.

It is the responsibility of the client to inform the relevant authorities in the event of a breach affecting personal data as required by the UK DPA or EU GDPR.