CE6014_Computer Mediated Communication
Information Security- Protection and Access of Data

Project Update Presentation

Lecturer: Assist.Prof.Dr. Matevž Dolenc

Student: Colin Perry

Institution: University College Cork

Date: 19th September 2018

Project Outline

With the collaboration and information sharing required for all projects but especially that required for a modern BIM project, protecting the data is paramount.

The data needs to be protected from unauthorised changes yet available to only those that should have access. It will also need to be available to those that need it for construction purposes, without the ability to change it.

The idea of people leaving some data in a briefcase is insignificant compared to loss of data through a data theft or corruption particularly of a BIM model.

This project will explore methods of ensuring the right people have access: Whom has access, how to provide sufficient access for those who need it,

I will review how home working and modern work methods can impact data security.

Change control

Taking a review of whom else has access to the data through software agreements and legislation.

With the modern society and our connected world how penetration testing of the network can assist in keeping data secure.

Exploring simple measures which can assist in preventing unauthorised users gaining access to systems. Access with two factor authentication and other secure measures.

ITC Euromaster
European Master Programme in Information Technology in Construction

Authorised Access:

Access to data is generally restricted. As the loss can be quite catastrophic.

Cyber security and ensuring only the right users have access.

Two factor authentication for users.

At the end of a user making changes make them add credentials again or changes are lost. Also periodically make them identify themselves if they are working for a prolonged period / no activity.

Dual password entry for administrative changes where two people know half the password.

The platform used whether cloud based or dedicated server.

Know what is in your agreements with any hosting company.

Many governments are enacting legislation similar to the US government's CLOUD act which enables them to request data from a provider located in their country whether the data is stored there or not.

Open to abuse by corrupt officials.

Penetration Testing:

```
$writeTime = Get-Date
$filePath = "C:\TEMP\#SITE# 131035 Internet Connectivity Test.log"
$nlm = [Activator]::CreateInstance([Type]::GetTypeFromCLSID([Guid]"{DCB00C01-570F-4A9B-8D69-199FDBA5723B}"))
$nlm.GetNetworkConnections() | ForEach-Object {
$output =[PSCustomObject]@{
NetworkName = ($_.GetNetwork().GetName());
ComputerName = $env:computername;
isConnectedToInternet = $_.isConnectedToInternet;
```

One measure which has been explored was whether it is possible to create code to verify active connection points are valid. It is possible in small networks with the code assembled in the project but not suitable for mid to large organisations.

This test is also limited in that the code could only detect active connections and therefore other tests would need to be applied to check for Bluetooth or wireless devices connected which at the time of the penetration test were not connected to an outside source.

Conclusions

Future Steps

- Select the system being created with care.
  - Ensure you are aware of hosting locations and legislation.
- Prevention is better than cure
  - Manage all users actively
  - Use two factor authentication
  - Have a system using user access tokens
- Major changes should require a split password. (Deletion/ Upload/ Model Transfer or change to major components)

- Complete the report in the current outline
- Continue to work on code for penetration testing

Project Outline

Table of Contents