CYBR373

Assignment 2

Olivia Fletcher
300534281
fletcholiv

Security Breach Review - Ministry of Social Development

Introduction

The Ministry of Social Development is a governmental body which provides services helping kiwis nationwide ensuring their job searching process is as seamless as possible. Due to the excessive amount of resources required to ensure customers needs are met the Ministry implemented Kiosks in the offices to help dampen the workload on employees. These kiosks are a tool, similar to an ordinary computer, whose prime use is supporting job seekers.

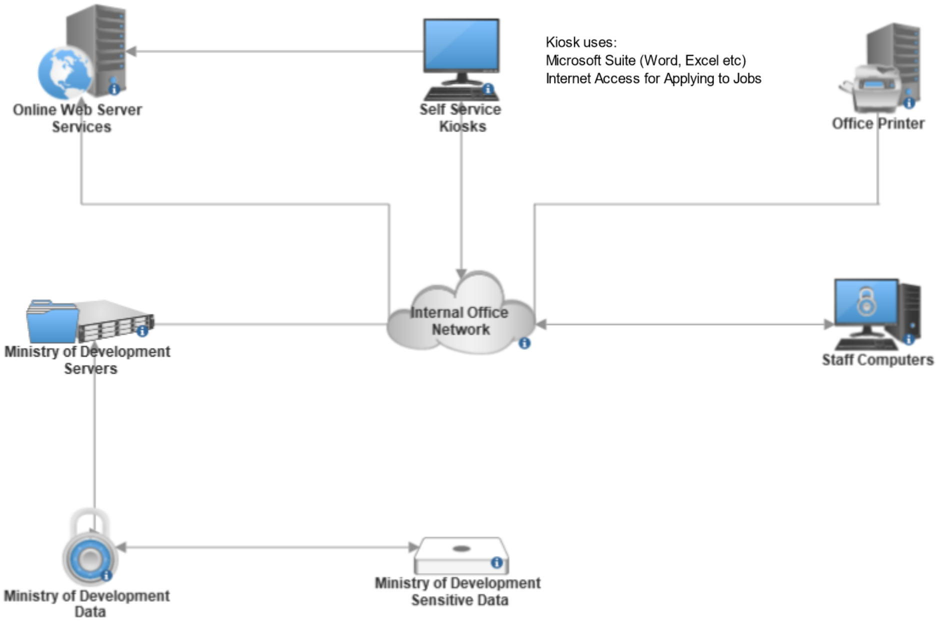
However, on the 14th of October 2012 the Ministries cybersecurity team was notified that an incident took place on a kiosk machine. The Ministry's information security had been breached, losing upwards to 7000 classified documents to the hands of an attacker. In this report we will be assessing the control strategies that the Ministry executed in dissipating this threat and what the processors will be to ensure this doesn't happen in the future.

Task 1

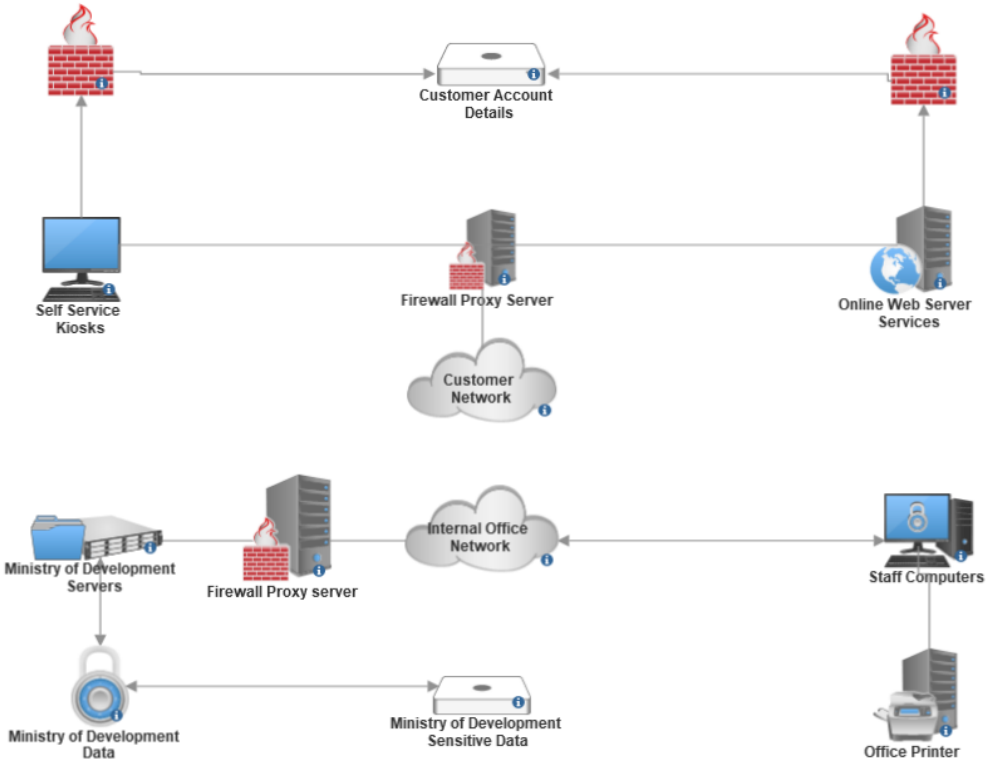
[5 Marks] Provide a network diagram figure highlighting the architecture of the Kiosk network and services. The figure must include the network topology, software and services running on the kiosk systems and servers, potential configurations and, the type of current security controls in place. (next page)

- Operation of the kiosks were available from 8:30 - 17:00 Monday, Tuesday, Thursdays, Fridays and 9:30 - 17:00 on Wednesdays
- The kiosks provide internet access, access for USB devices, Microsoft office applications for CV/letter creation and printing capabilities

- Current topology shows that the Kiosks are connected to the same office network that the sensitive data is connected to.


Online Web Server Services
Self Service Kiosks
Kiosk uses:
Microsoft Suite (Word, Excel etc)
Internet Access for Applying to Jobs
Office Printer
Internal Office Network
Ministry of Development Servers
Staff Computers
Ministry of Development Data
Ministry of Development Sensitive Data

- A proposed topology where the Kiosks are disconnected to the Ministry of Developments network with added firewall protection.



Task 2

[5 Marks] List and briefly explain the containment strategy, Incident Response (IR) and Disaster Recovery (DR) actions taken by the Ministry in response to the incident. This should include actions taken by all incident handlers on this incident.

Containment Strategy; [Reference 1]

Date	Event
02/22/2011	The IT security team requests more information from Mr Brereton including the date of which he discovered this issue. The IT team was unable to replicate the issue.
10/10/2012	The ministry contracts out for penetration testing on all of its websites.
11/10/2012	The ministry makes changes to the web applications from the assumptions from Mr Brerertons cryptic messages.
14/10/2012	Mr Ng notifies the Privacy Commissioner about the security breach and informs the media, Radio New Zealand about the breach.
15/10/2012	The ministry announces that they will do an independent review on the breach. Mr Ng provides the ministry with a USB device which contains all the sensitive information he was able to gather on the kiosk machines. The ministry then investigated the USB device contents to determine the potential impacts the leaked data could contain.
16/10/2012	The Ministry employs Deloitte as an independent reviewer of the kiosk data breach. The ministry works on developing strategies into making the kiosks more secure.

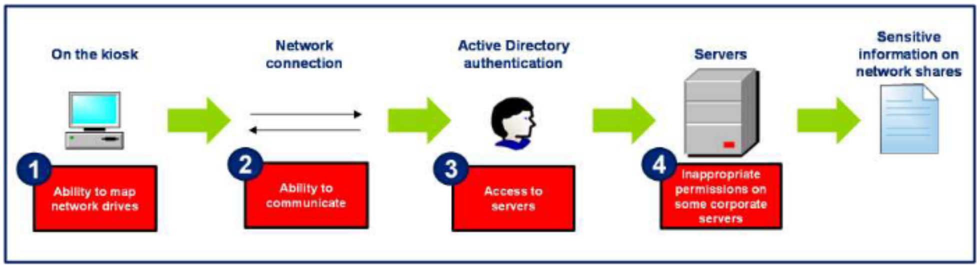
Incident Response; [Reference 2]

Date	Event
10/10/2011	Ms Brereton raises a concern with the kiosks and demonstrates that she is able to access sensitive files. The issue is discussed with the staff.
01/11/2011	Ms Brereton raises the information issue disclosure on the kiosks to the senior business manager. Issue was forwarded to the ministry to be investigated.
29/11/2011	Work and Income query the IT security team on the issue.
05/10/2012	Mr Bailey uses a kiosk and discovers that he is able to directly connect to the corporate network and can map network drives and files.
08/10/2012	The Ministry attempts to gain further information from Mr Bailey regarding the breach and he declines. Mr Bailey informs Mr Ng of the security vulnerability.
14/10/2012	The Ministry's actions were to disable the kiosk machines, restrict server permissions on all of Mr Ng’s accounts and to change the kiosk settings.
17/10/2012	Deloitte begins its review on the breach.wdqsdfdsfsrdcv

Disaster Recovery; [Reference 3]

Date	Event
Late 2012	The Deloitte review team communicated further with Ms Brereton to gather more information. Ms Brererton suggested that the issue may be potentially related to the way the IP connections are deployed on the kiosks through the office network. The Ministry concluded from their conversation that there is no evidence that Ms Brererton had gained access to any private Ministry data.
Late 2012	The Deloitte review team interviewed Mr Bailey and Mr Ng. After forensically investigating the contents of the USB drive they discovered that of the 7307 copied files in total contained 533 CERA invoices. CERA has been notified of the incident and are dealing with the implications of this breach for each item copied.
Late 2012	The final 6777 files contained the Ministries accounting information such as private invoices of clients including their full names, addresses, phone numbers, financials and medical information.
Late 2012	Deloitte concurred that the breach happened due to four technicality issues in regards to the kiosks. - The kiosks did not have adequate access privilege rules and thus the ability to map network drives was not restricted. - The kiosks are directly connected to the Ministry's corporate network which also did not contain any firewall or preventative measures in case of a breach. - Any client using the kiosks had default privileges on line with being an already authenticated user on the Active Directory network domain. This meant that users had access to shared drives on the network. - Shared files on the Ministry network were not assigned appropriate access privileges.
15/10/2012 - 30/10/2012	Through discussion with Mr Bailey the Ministry confirmed that he has not retained any of the stolen data. The ministry retrieved the USB drive from Mr Ng. Mr Ng signed a statutory declaration which confirms that he no longer has the Ministry's data in possession of which he gathered from the Kiosk breach. With attempts made by the Ministry for Mr Bailey to sign the declaration he has declined but gave his verbal assurance that he no longer has possession of the documents.

How the breach took place - Figure from Deloitte Independent Review


On the kiosk
Network connection
Active Directory authentication
Servers
Sensitive information on network shares
1
Ability to map network drives
2
Ability to communicate
3
Access to servers
4
Inappropriate permissions on some corporate servers

Task 3

[30 Marks] Citing NIST SP.800-61, NIST SP.800-53 and NZISM (2) and/or other relevant NIST documents, discuss in details how the vulnerabilities in the physical and logical design and architecture of kiosk can be mitigated or minimized by application of physical and technical controls:

a. Deterrent, detective and preventive controls (e.g Banners, locks, CCTV, access control, encryption, packet filtering, HIDPS, NIDPS, audits and logs etc)

Deterrent;

Citing	Name	Description
NIST SP 800-53 3.1 AC-1 [4]	Access Control Policy	In a governmental business such as the Ministry which handles sensitive public data it is vital to have an adequate access control policy in place. In the NIST AC-1 section it states that having an access policy which has the appropriate ACL rules in place can deter malicious intent simply by not allowing access to unauthorized individuals.
NIST SP 800-53 3.1 AC-2 [4]	Access Control Policy	Designate and assign an IT professional whose job is to manage and maintain the access control rules and procedures. This would be an important measure for someone to monitor public usage of the Kiosk devices and/or networking
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Define appropriate directory/file read/write/execute privileges to the associated accounts. (e.g, client users only have read/write/execute privileges on their own files.)
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Only assign account managers for system accounts that contain sensitive data and establish conditions for the group users and roles. This would help deter any potential data breach that could happen in the Ministry.
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Enforce that every worker or contractor entity hired by the ministry meets secure account standards. Must have a minimum password requirement and have 2FA enabled.
NIST SP 800-53 3.1 AC-3 [4]	Access Enforcement	Enforce the mandatory access control policy over all occupants of the Ministry and third party connections in all cases such as; - When data is sent through the public/private networks - When data is being shared to other occupants - Fully document when an individual has been authorized to behave outside of their bounds of permissions (such as passing data to someone without authorization to said data).
NIST SP 800-84 3.1.2 [5]	Information Flow Enforcement	Use protected processing domains to enforce the already in place policies for the ministry's internal information flow. Prevent encrypted information from being passed within the networks by using an automated blocking system.

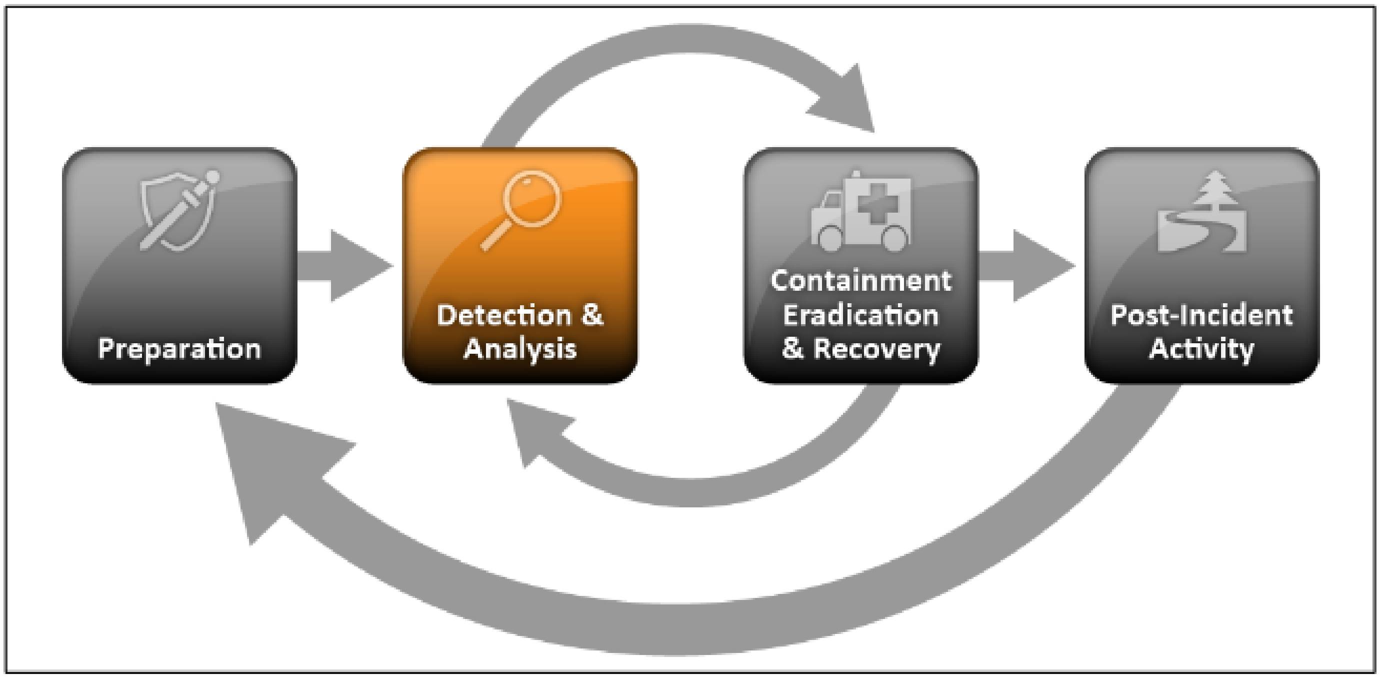
Detective;

Citing	Name	Description
NIST SP 800-53 3.1 AC-1 [4]	Access Control Policy	Create a routine review process which is responsible for assessing current access control rules and to update accordingly.
NIST SP 800-53 3.1 AC-1 [4]	Access Control Policy	Routinely monitor the use of administrative system access control policies.
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Enforce conditions for account management. Guidance from NIST AC2 Account Management section 11 & 12 states that the use of monitoring system accounts such as time usage and system access pattern analysis to determine any ill intent or suspicious activity. Section 11 states that enforcing specific guidelines for account usages and limited information to certain dates/times decreases the likelihood of an account data breach.
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Similar to the access control policy, to monitor every time an authorized subject accesses sensitive system data and information and records the files used by the subject.
NIST SP 800-84 3.1.2 [5]	User Awareness and Training	Ensuring when taking in third-party contractors and hired workers that they have had adequate training in risk assessments, threat prevention and general awareness. Having a guard on premise whose job is to physically monitor the clients using the kiosks/public services to ensure no malicious intent is taking place.
NIST SP 800-84 3.1.2 [5]	Malware Prevention/ Network Security	Having an alarm system on the network devices which alerts the system administrators of a potential virus/breach. Ensuring all network firewall and antivirus is up to date with degular checks to monitor it's effectiveness.
NIST SP 800-84 AC-9 [5]	Previous Login Access Notification	Having a log system in place where clients get notified every time their account has been accessed/where it was accessed and what information was accessed on their account. The client should be able to access their previous account logs as-well and have a contact-line at the ministry specifically for the case of a potential account breach.

Preventative;

Citing	Name	Description
NIST SP 800-53 3.1 AC-1 [4]	Access Control Policy	Create a distinct remediation plan in case of access control violations. Including an automated mechanism which notifies management/whoever is in charge of the controls to update the roles after an employment has been terminated and after every term or so.
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Define appropriate directory/file read/write/execute privileges to the associated accounts. (e.g, client users only have read/write/execute privileges on their own files.)
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Require approvals to access administrative accounts by the staff member that monitors the system log-ins.
NIST SP 800-53 3.1 AC-3 [4]	Access Enforcement	Configure for a dual authorization so that two authorized working individuals at the ministry are required for approval when requesting system entry.
NIST SP 800-53 3.1 AC-3 [4]	Access Enforcement	Create a policy where when a trusted individual is attempting to send data to another party where the receiving party does not have the valid permissions in place to access said data there will be a blocking.

Detection Analysis - Figure from NIST SP 800-53



b. Responsive and corrective controls (e.g removal of malicious files by an antivirus, backups etc.)

Responsive;

Citing	Name	Description
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Review and update the role account privileges routinely when; - Every term/month or when appropriate - Users are terminated or transferred - When accounts are no longer needed - When suspicious of an individual's access to system information
NIST SP 800-53 3.1 AC-2 [4]	Account Management	Temporary disable accounts of users who could pose significant risk of data breach and could be a part of a group where the incident took place. Keep the account spreviledges disabled until the investigation concludes each user's account history and has been set as clear.
NIST SP 800-84 3.1.2 [5]	Preventing Incidents	Risk assessments - Having a definitive plan for periodic risk assessments of software, policies and privilege roles to assess the potential threats or breaches
NIST SP 800-84 3.1.2 [5]	Preventing Incidents	Malware Protection. Ensuring the antivirus on all network devices and clouds are up to date and checked regularly.
NIST SP 800-84 2.6 [5]	Preparation	Ensure that at any moment of time that the ministry is always adequately prepared for a potential threat to take place and is able to immediately remediate the concern.
NIST SP 800-84 AC-7 [5]	Unsuccessful Login Attempts	Enforce a limit of unsuccessful login attempts for clients using ministry devices and have a response plan where the IT security team gets notified of the attempted account that has failed attempts and which/where the kiosk location is.
NIST SP 800-84 AC-23 [5]	Data Mining Protection	Because clients have access to USB on the kiosks and public devices offered at the ministry it is important to employ a strategy to avoid malicious intent of a user inputting keyloggers, data mining and malware on the devices.

Corrective;

Citing	Name	Description
NIST SP 800-84 2.6 [5]	Incident Response	Establish a matriculate incident response plan for groups of potential risk factors such as; in case of a kiosk breach, public network breach, physical damage to ministry property etc. If an incident were to take place and the correct incident response plan was followed it would allow for less potential damages to the ministry.
NIST SP 800-84 AC-5 [5]	Separation of Duties	By separating duties and responsibilities it ensures that when facing a threat at hand the ministry employee structure remains organized and makes it easier to perform plans in correcting the threat.
NIST SP 800-84 AC-9 [5]	Previous Login Access Notification	Similar to the detective section, in the case where a client has been notified of a successful login to their account they should have the ability to log out to be able to lock the access to their account in case of an attacker gaining information on the client. Having a contact-line specifically for account breaches at the ministry so that these can be immediately sorted to avoid a data leak.
NIST SP 800-84 AC-11 [5]	Device Lock	Adding onto the ‘previous login access notification’ to be able to prevent further access to the system where the ministry can lock client accounts or ministry system accounts. Having an automated system where if any suspicious activity has been detected to automatically lock the session and notify the IT department to investigate further.
NIST SP 800-84 AC-16 [5]	Security and Privacy Attributes	Audit changes to security and privacy attributes. When a threat takes place after an investigation has taken place and the threat location has been identified to make full security changes to ensure this doesn’t happen again.

References

[1] Final report - Phase 1 - Deloitte, page 6
[1] Final report - Phase 1 - Deloitte, page 16-19
[3] Final report - Phase 1 - Deloitte, page 26-32

[4] Security and Privacy Controls for Information Systems and Organizations, National Institute of Technology, U.S Department of Commerce, NIST Special Publication 800-53, pages 17-25

[5] “Computer Security Incident Handling Guide”, Paul.C, Tom.M, Tim.G, Karen.S, National Institute of Standards and Technology U.S Department of Commerce, NIST Special Publication 800-61, pages 19-24, http://dx.doi.org/10.6028/NIST.SP.800-61r2