Vol.2018-CSEC-81 No.25
Vol.2018-IOT-41 No.25
2018/5/18

The Beast that Shouted Governance at the Heart of the University

Hiroki Kashiwazaki[1,a)]

Abstract: In December 2017, a Japanese university announced large-scale personal information leak. According to open information, the leak was caused on several systems by several unauthorized accesses. Also in February 2018, a Japanese research institute announced a large-scale security incident. Even only in Japan, many reports of cyber security incidents are announced for a year. After security incidents occur, a supervisory agency (in these cases, Ministry of Education, Culture, Sports, Science and Technology a.k.a MEXT) and security advisory consulting companies order the institutes to "strengthen governance in their own institutes". This paper shows an example of personal information leak incident in an university and a beast that asked what is the governance in the university at the heart of the university.

1. Introduction

A lot of security incidents on research and educational institutes are reported. As for incidents for university, GhostShell university hack in 2012[*1] is one of the most well-known and worst example. Project WestWind, that Team GhostShell called their campaign, is aimed at "raising awareness towards the changes made in today's education, how new laws imposed by politicians affect us, our economy and overall, our way of life". Records stolen from university databases were made publicly available with link tweeted to the release posted on Pastebin[*2]. The records included 36,623 unique email addresses, tens of thousands of student, faculty, staff names, thousands of usernames, hashed and plain-text passwords, addresses, phone numbers and database schema information. Sensitive information including dates of birth, citizenship, ethnicity, marital status and gender was also included.

Japanese research and educational institutes, University of Tokyo, Kyoto University, Tohoku University, Nagoya University and Osaka City University are included in victims of GhostShell. Although targets of GhostShell were 100 top universities, the reason why Osaka City University was targeted was that the team could be false to recognize Osaka University and Osaka City University. After the Project WestWind, security incidents on Japanese research and educational institutes are classified to unauthorized accesses (led by phishing, weak passwords, brute force attack and so on), malware infections and Denial of Services (DoS). Both unauthorized accesses and malware infections can result in personal or confidential information leak.

In this two years, one of the most notorious information leak was occurred in Toyama University. According to the incident report[*3], Toyama university have never recognized the fact of the incident until external institute told the fact to the university. A trigger of the incident was targeted email attack. The incident of Hokkaido University was unauthorized accesses that was recognized by mass mailings from an internal host to a lot of external recipients[*4]. Because the host served file service, information leak could be suspected. But according to the reports, the suspicion was denied. After these incidents, all of national universities and research institutes were obliged to make Computer Emergency (or Security Incident) Response Team (CERT or CSIRT) in their own organization by the end of March, 2017, by order of MEXT, the ministry that has responsibility to supervise national universities and research institutes.

In 2018, National institute of advanced industrial science and technology (AIST) released security incident brief report on February[*5]. The incident was caused by unauthorized access of widely used SaaS service, Office365[*6]. AIST decided to shut down their internet connectivity. And the shutdown continued at least until 15, March[*7]. Now, the author would like to talk about a certain Japanese university, that has more than 23 thousand students (including graduate students, Ph.D candidates), more than 3 thousand research staffs and 6 thousand administration staffs (including part time staffs). What was happen in the university and how members of CERT in the university act against the incident are described in the next section according to published information.

[1] Cybermedia Center, Osaka University, Ibaraki, Osaka, 567–0047, Japan
[a)] reo@cmc.osaka-u.ac.jp

[*1] https://www.zdnet.com/article/ghostshell-university-hack-by-the-numbers/
[*2] https://pastebin.com/
[*3] https://www.u-toyama.ac.jp/news/2016/1011.html
[*4] https://www.hokudai.ac.jp/news/2016/01/post-377.html
[*5] http://www.aist.go.jp/aist_j/news/announce/au20180213.html
[*6] https://www.office.com/
[*7] http://www.security-next.com/091178

2. An example of a CERTAIN university

A certain university had a press conference on 13 December, 2017 and some newspaper and broadcast company distributed summarized contents of the press[*8]. Piyokango[*9], who is the most reliable cyber security journalist in Japan, summarized the incident according to the published sources[*10]. According to the article, timeline of the incidents are shown in Table.1.

Table 1 Timeline of the incident.

date	detail of timeline
18th May to 4th July	Unauthorized accesses occurred in internal information systems in a certain university.
21th June	The university recognized unauthorized accesses.
(N/A)	The university asked a external security company for a survey of the accesses.
(N/A)	Surveillance team discovered analysis programs that were seemed to be deployed by unauthorized users.
25th July	The university considered that there were exactly unauthorized accesses to the internal systems.
1st Aug. to 28th	The university implemented measures to prevent recurrence against unauthorized accesses.
13th Dec.	The university made a press conference, announcing that there is a possibility of unauthorized accesses and information leakage.

The university also announced that secondary damage was not confirmed and leaked information did not include patient information of a medical hospital in the university.

The incident can be classified (and also were explained in the press conference) to three stages. First stage is the "users". The users include students, administration staffs and research staffs, who has credential information of the university. They always face a threat of stealing credentials with phishing. Second stage is an "educational computer system". Last stage is a "groupware system". As for the first stage, according to the press information, credentials of a research staff was stolen by malicious users but the university did not explain how they steal. The university introduced single sign-on (SSO) system. The malicious users could access to some systems that were collaborate with the SSO system. The staff did not have any administrator privileges. All of IPv4 addresses that the malicious users accesses from are owned by foreign country organizations.

2.1 Educational computer system

The educational information system of the university are used for e-mail, browsing, programming, and other similar functions in order to provide consistent information technology support for the educational curriculum. Computer assisted language learning system is also a part of the system. The system consists of approximately 1200 computers that are connected to the university information network. The system provides not only IT environment and language learning but also cultural studies.

According to Piyokango's article, the timeline of the stage of the educational computer system is shown below.

(1) The malicious user who stole the credential of the staff compromised the educational computer system with the credential stolen.
(2) The malicious user deployed (cloned) malicious programs[*11].
(3) The malicious user succeeded to sniff and crack credentials of administrator users.
(4) The malicious user accessed to (general) user information in the system.

The contents of "user information" are different between each user group. According to the publication of the university, the classified leaked user information and their amount is shown in Table.2.

Table 2 Leaked information in the educational computer system.

group	amount	contents of leaked information
staffs[*12]	12,451	UID, name, affiliation, E-mail address[*13].
students	24,196	UID, name, affiliation, E-mail address, year of entrance, student ID[*14].
former staffs	9,435	UID, name, affiliation, E-mail address.
former students	23,467	UID, name, affiliation, E-mail address, year of entrance, student ID.

ID and E-mail address of former staffs and former students were obsoleted at the time of the press conference.

2.2 Groupware system

Groupware system is a groupware that shares information and communicates information among staffs of the university. Information that should be shared by all faculty and staffs, such as university events, announcements, notifications, etc., are posted to the system. Groupware system is a Web system so user can access from anywhere with the browser.

Also according to Piyokango's article, the timeline of the stage of the Group system is shown below.

(1) The malicious user compromised the Groupware system with 59 users credentials that are cracked in the Educational computer system.
(2) The malicious user can read E-mail of 59 users that include personal information with attached files.

The leakage of the personal information are not observed but can be. According to the publications of the university, the personal information that could be leaked from the Groupware was very various and huge. The owner of leaked information can be classified to two groups, insider of the university and outsider. The contents of leaked information of insider are shown in Table.3, the contents of outsider are shown in Table.4.

Total amount of "potentially" leaked information was more than 11 thousand both insiders and outsiders.

2.3 Question marks

Although the publication of the university was sincere and its description is in detail, my intelligent readers may mind a lot of questions like these:

- How the malicious users can steal a credential of the research

[*8] A company exaggerated. I will never forgive N■K, never.
[*9] https://twitter.com/piyokango
[*10] http://d.hatena.ne.jp/Kango/?of=13
[*11] cf) https://github.com/gentilkiwi/mimikatz

Table 3 Leaked information of insiders from the Groupware system.

source	amount	contents of leaked information
miscellaneous mail body and attached files	1,008	name, affiliation, job title, telephone number, E-mail address.
spreadsheets for internal works	211	name, birth date, affiliation, job title, UID.
spreadsheets for internal works (social insurance)	591	name, birth date, UID, standard monthly income, social insurance premium.
list of emergency contact	252	name, affiliation, job title, phone numbers[*15].
application forms of UID	469	name, birth date.
application forms of systems	1,055	name, UID, E-mail address.

Table 4 Leaked information of outsiders from the Groupware system.

source	amount	contents of leaked information
miscellaneous body of mails and its attached files	6,042	name, affiliation, job title, address, telephone number, E-mail address.
replied mail to query	376	name, affiliation, telephone number, E-mail address.
lists of those who passed exam in certain test.	54	name, birth date, address, telephone number, mail address, academic records.
lists of job applicants	30	name, birth date, address, mail address, academic records, work records.
mail with other organizations	420	name, affiliation, telephone number, mail address.
lists concerning to the event	12	name, affiliation, address, telephone number, mail address.
participants list of an event (1)	30	name, affiliation.
participants list of an event (2)	86	name, telephone number, E-mail address.
participants list of an event (3)	30	name, affiliation, telephone number, E-mail address.
participants list of an event (4)	25	name, affiliation.
lists of donators.	367	name, address, telephone number, E-mail address.
lists of publication distribution	500	name, affiliation, address, E-mail address.

staff in the stage of "users"? [*16]

- What on earth are excellent programs that can sniff and crack the credentials of administrators in a short period.
- Whether the causation of each incident stage are clear or not.

The "intelligent" university may "intentionally" describe these points ambiguously. However that may be, members of CERT in the university had to determine the way to clean up the incident, because MEXT had been very angry.

3. Cleanups of the incident

It is worth noting in Table.1 that the long period between 28th August and 13th December. Although the author cannot refer to the reason why the period was needed to publish because of confidentiality for information that may become known in the course of business, the author can refer to the present IT activities in the university. The author does not refer whether these activities are preventive measures for recurrence or not.

- Enlargement of the amount of stored various logs generated from IT systems and network equipment.
- Introducing and operation of next generation endpoint security solutions.
- Establishment of steady and frequent operation to maintain security level.
- Organization reform to be able to respond to security incidents.

Specific design and preliminary calculation of some of these activities are shown below.

3.1 Storage for PB scale log files

In the university, total amount of log of firewall equipment on the interface between SINET5[*17] and the university network was limited. Because of the limitation, log information did not help to reveal causation and deny suspicion of other malicious activities after the incidents. The university has 100 Gbps connection to the SINET5. The actual averaged throughput is approximately several Gbps. MEXT ordered the university to store traffic logs at least for a year. Total amount of storage T required is led by the equation shown below if the averaged throughput is t Gbps if all traffic is recorded.

$$\begin{aligned} T(\frac{TB}{year}) &= t(\frac{Gbit}{sec}) \times 60(\frac{sec}{min}) \times 60(\frac{min}{hour}) \times 24(\frac{hour}{day}) \\ &\quad \times 365(\frac{day}{year}) \div 8(\frac{bit}{Byte}) \div 1024(\frac{GB}{TB}) \\ &\sim 3850 \times t \end{aligned} \tag{1}$$

Thus, approximately PB scale storage is necessary to store all the traffic if the average traffic is even several Gbps. But full payload are not necessarily required. According to the result of survey for the Internet mixture (IMIX) [1], distribution of packet size in the Internet traffic is biased both side of smaller than 100 bytes and larger than 1,300 bytes. After the survey, video traffic grow larger than before according to Cisco Visual Networking Index[*18]. According to the sources, packets larger than 1,300 bytes are supposed to be dominant in the present status of network. If traffic log is stored only Layer 2, 3 and 4 headers and a certain head part of payload, storage size can be reduced to one tenth of full stored size.

3.2 Steady scans for vulnerabilities

After the unauthorized access, horizontal privilege escalation is one of threats. If the servers in the university expose their vulnerability, horizontal privilege escalation can be easily done. To prevent the increment of the (impact) amount caused by vulnerabilities in the university, the university decided to introduce a integrated vulnerability scanner solution "tenable.io"[*19] from Tenable[*20] via TOYO Corporation[*21]. Tenable.io is an integrated

[*16] The university gave "unknown" as the answered to the question.

[*17] Science Information NETwork 5, operated by National Institute of Informatics. https://www.sinet.ad.jp/

[*18] https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

[*19] https://www.tenable.com/products/tenable-io

[*20] https://www.tenable.com/

[*21] https://www.toyo.co.jp/english/

platform that can control products of Tenable such as Nessus. According to the white paper, it brings clarity to security of the organization and compliance posture through a fresh, asset-based approach that accurately tracks resources of the organization and vulnerabilities, while accommodating dynamic assets like cloud and containers. it can maximize visibility and insight and effectively prioritizes the vulnerabilities, while seamlessly integrating into environment of the organization.

At the early stage after introducing Tenable.io to the university, the operations of scanning vulnerability are executed manually with Web interface. But manual operation occurred some mistakes ant its human cost is pretty large. By using Tenable.io API, the author have been making and published an object oriented design of Tenable.io by Ruby[*22] correspond to Tenable.io API design[*23]. According the class library, a large part of operations were changed to be programmable and programmable procedure could reduce the human cost.

4. What is governance for universities?

After the incident, MEXT frequently told the university to "strengthen governance", "improve governance" and "activate governance". The author wondered if MEXT staff would get a "governance" disease. So the author also wondered what is the meaning of, or definition of "governance"? Yanase Naoki (1943-2016), who was one of the greatest translator in Japan and whom the author respects deeply, told that "Hence dictionaries. Dictionaries are given to ordinary people" [2]. According to Oxford English Dictionary, the definition of the word "governance" is that "The office, function, or power of governing; authority or permission to govern". Then next, what is the definition "govern"? According to the dictionary, the definition of "govern" (verb) is that "To oversee or have responsibility for (a person, esp. a child); to be the guardian or patron of; to keep safe, protect" or "To hold or exercise personal authority over (a person, esp. a child); to exert proper or fitting control over; to discipline".

Meanwhile, some researchers such as Mark Bevir[*24] notes the definition is obsolete. What he told in his book is shown below [3].

Mark Bevir: Governance: A Very Short Introduction

'Governance' might appear to be a weasel word – a vague euphemism for government. Other sceptics believe that the word 'governance' is used so widely that it has become tired. Discussions of governance occur in diverse contexts and disciplines, including development studies, economics, geography, international relations, planning, political science, public administration, and sociology. Too little attention is given to ways of making sense of the whole literature on governance.

Governance differs from government both theoretically and empirically. In theoretical terms, governance is the process of governing. It is what governments do to their citizens. But it is also what corporations and other organizations do to their employees and members. Further, the process of governing need not be consciously undertaken by a hierarchically organized set of actors. Markets and networks of actors can govern, produce coordination, and make decisions. Whereas government refers to political institutions, governance refers to processes of rule wherever they occur.

(snip)

Governance can refer abstractly to all processes of governing. It supplements a focus on the formal institutions of government with recognition of more diverse activities that blur the boundary of state and society. It draws attention to the complex processes and interactions involved in governing. Governance can also refer, more concretely, to the rise of new processes of governing that are hybrid and multi-jurisdictional with plural stakeholders working together in networks. It describes recent changes in the world.

The topology of universities is far from tree structure. The meaning and the way of being "governance" may be quite different from ones of top-down organizations. Now is the time that researchers in universities start to find the way of being the governance in the university from the aspect of science.

5. Conclusion

This paper shows an example of cyber exposure and information leak in a certain university. Several attempts to prevent recurrence are also described. The author brings up an issue for the way of being governance in universities. More detailed and vivid explanation of the incident may be presented in the IOT41 meeting.

[*22] https://github.com/reokashiwa/tenable
[*23] https://cloud.tenable.com/api
[*24] http://polisci.berkeley.edu/people/faculty

References

[1] Murray, D. and Koziniec, T.: The state of enterprise network traffic in 2012, *2012 18th Asia-Pacific Conference on Communications (APCC)*, pp. 179–184 (online), DOI: 10.1109/APCC.2012.6388126 (2012).
[2] Yanase, N.: *Joyce full dictionary (Mass Market Paperback) (1996) ISBN: 4101480117 [Japanese Import]*, Shinchosha (1996).
[3] Bevir, M.: *Governance: A Very Short Introduction (Very Short Introductions)*, OUP Oxford (2012).