Document Summary

AOT ICT Vulnerability Assessment and Penetration Test Report

The document is the AOT results of ICT vulnerability assessment and penetration by a third party, Asian Intelligent Information Technology (AIIT).

Table of content

เอกสารลับ

โครงการงานจ้างตรวจสอบและประเมินความปลอดภัย
ของเครื่องคอมพิวเตอร์แม่ข่าย เลขที่สัญญา 1CH10-630013

บริษัท ท่าอากาศยานไทย จำกัด (มหาชน)
(Airports of Thailand)

รายงานผลการดำเนินการตรวจสอบและข้อเสนอแนะในการปรับปรุงแก้ไขระบบ

(สำหรับผู้ดูแลระบบ)

บริษัท เอเชี่ยน อินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด
Asian Intelligent Information Technology Co., Ltd. (AIIT)

สารบัญ

เรื่อง **หน้า**

1. ขอบเขตและข้อมูลโดยสรุป (Scope and Summary)

ตามที่บริษัทเอเชี่ยน อินเทลลีเจนท์ อินฟอร์เมชั่น เทคโนโลยี จำกัด ได้ดำเนินการประเมินความเสี่ยงและทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ให้กับ บริษัท ท่าอากาศยานไทย จำกัด (มหาชน) มีวัตถุประสงค์เพื่อ

- ระบุช่องโหว่และการโจมตีที่มีอยู่ของ ทอท.
- ปรับปรุงค่าความปลอดภัยของข้อมูลโดยรวมของ ทอท.
- ประเมินความเสี่ยงจากผู้ประสงค์ร้ายที่ต้องการการเข้าถึงเครือข่าย ทอท.
- ให้คำแนะนำในการแก้ไขช่องโหว่ สำหรับการรักษาความปลอดภัยข้อมูลในอนาคต

1.1. วิธีการตรวจสอบช่องโหว่ของระบบ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) (Approach)

ทางบริษัทได้ทำการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) โดยใช้วิธีการมาตรฐานสากล (Common Vulnerability Scoring System – CVSS) ในการประเมินความเสี่ยงให้กับทาง ทอท. ซึ่งได้มีการปรับเกณฑ์ให้เข้ากับระบบปัจจุบันและสภาพแวดล้อมของ ทอท. ตามความเหมาะสม

1.2. ขอบเขต (Scope)

ก่อนดำเนินการตรวจสอบช่องโหว่ (Vulnerability Assessment) และทดสอบเจาะระบบ (Penetration Testing) ทาง ทอท. ได้ส่งมอบข้อมูลด้านล่างเพื่อใช้เป็นข้อมูลประกอบในการดำเนินการต่างๆ ตามขอบเขตของงาน

No	Testing approach	IP	System	Execution time	Execution date
1	External	110.170.118.69	Web Disp DEV/QAS	13.00 - 17.00	2 มีนาคม 2563
2	External	110.170.118.61	SAP Router PRD		2 มีนาคม 2563
3	External	110.170.118.70	Web Dispatcher PRD #1		2 มีนาคม 2563
4	External	110.170.118.71	Web Recruit		2 มีนาคม 2563
5	External	110.170.118.72	safety.airportthai.co.th.	09.00 - 17.00	3 มีนาคม 2563
6	External	110.170.118.52	api.airportthai.co.th.		3 มีนาคม 2563
7	External	110.170.118.62	cmms.airportthai.co.th.		3 มีนาคม 2563

No	Testing approach	IP	System	Execution time	Execution date
8	External	110.170.118.22	mobile.airportthai.co.th.		3 มีนาคม 2563
9	Internal	10.74.29.63	CMS-UMGP1	09.00 - 17.00	4 มีนาคม 2563
10	Internal	10.74.29.226	LINEAPP-API		4 มีนาคม 2563
11	Internal	10.74.29.225	LINEAPP-APP		4 มีนาคม 2563
12	Internal	10.121.1.130	LINEAPP-DB		4 มีนาคม 2563
13	Internal	10.74.29.163	mobile.airportthai.co.th		4 มีนาคม 2563
14	Internal	10.74.27.120	Integretionserver		4 มีนาคม 2563
15	Internal	10.74.26.161	E-security-dev-mobile		4 มีนาคม 2563
16	Internal	10.74.29.33	ESAFETY-DB		4 มีนาคม 2563
17	Internal	10.74.29.232	ESAFETY-APP		4 มีนาคม 2563
18	Internal	10.74.29.101	Web Disp DEV/QAS		4 มีนาคม 2563
19	Internal	10.74.29.102	SAP Router PRD		4 มีนาคม 2563
20	Internal	10.74.29.103	Web Dispatcher PRD #1		4 มีนาคม 2563
21	Internal	10.74.29.107	NFS Server WDP		4 มีนาคม 2563
22	Internal	10.74.29.108	Proxy for PO Server		4 มีนาคม 2563
23	Internal	10.121.3.119	SAP PO PRD		4 มีนาคม 2563
24	Internal	10.121.3.127	FTP Server DEV/QAS/PRD		4 มีนาคม 2563
25	Internal	10.121.3.142	Web RIC PRD1		4 มีนาคม 2563
26	Internal	10.121.3.123	SAP IDM PRD		4 มีนาคม 2563
27	Internal	10.74.236.20	Project Share		4 มีนาคม 2563

No	Testing approach	IP	System	Execution time	Execution date
28	Internal	10.74.236.21	Web Recruit APP		4 มีนาคม 2563
29	Internal	10.74.236.22	Web Recruit DB		4 มีนาคม 2563
30	Baseline	10.74.29.175	E-Payment		4 มีนาคม 2563
31	Baseline	10.74.29.63	CMS-UMGP1		4 มีนาคม 2563
32	Internal	10.74.29.230	Elearning-App	00.00 - 04.00	6 มีนาคม 2563
33	Internal	10.74.29.231	Elearning-DB		6 มีนาคม 2563
34	Internal	10.240.194.45	EDOCUMENT-APP01		6 มีนาคม 2563
35	Internal	10.240.194.46	EDOCUMENT-APP02		6 มีนาคม 2563
36	Internal	10.240.194.47	EDOCUMENT-FILE		6 มีนาคม 2563
37	Internal	10.240.194.92	PORTAL-WEB01		6 มีนาคม 2563
38	Internal	10.240.194.93	PORTAL-WEB02		6 มีนาคม 2563
39	Internal	10.240.194.94	PORTAL-WEB03		6 มีนาคม 2563
40	Internal	10.240.214.90	PORTAL DB		6 มีนาคม 2563
41	Internal	10.240.194.162	DC2-ADFSPROXY01		6 มีนาคม 2563
42	Internal	10.240.194.163	DC2-ADFSPROXY02		6 มีนาคม 2563
43	Internal	10.240.194.160	DC2-DNSSEC01		6 มีนาคม 2563
44	Internal	10.240.194.161	DC2-DNSSEC02		6 มีนาคม 2563
45	Internal	10.74.29.215	DC1-DNSSEC01		6 มีนาคม 2563
46	Internal	10.74.29.216	DC1-DNSSEC02		6 มีนาคม 2563
47	Internal	10.74.29.160	aitside		6 มีนาคม 2563

No	Testing approach	IP	System	Execution time	Execution date
			traning.airportthai.co.th		
48	Internal	10.74.27.55	aitrside-cbt		6 มีนาคม 2563
49	Internal	10.74.27.89	astraning		6 มีนาคม 2563
50	Internal	10.74.29.72	ADPORTAL		6 มีนาคม 2563
51	Baseline	10.74.29.72	ADPORTAL		6 มีนาคม 2563
52	Internal	10.121.1.107	Carparkmain		6 มีนาคม 2563
53	Internal	10.121.1.207	Carparkdr		6 มีนาคม 2563
54	Internal	10.121.1.151	Carparkfreezonemain		6 มีนาคม 2563
55	Internal	10.121.1.152	Carparkfreezonedr		6 มีนาคม 2563
56	Internal	10.74.29.51	IMED-APP01	02.00 - 04.00	6 มีนาคม 2563
57	Internal	10.74.29.52	IMED-APP02		6 มีนาคม 2563
58	Internal	10.121.0.81	imeddb		6 มีนาคม 2563
59	Internal	10.74.27.127	imedinterface		6 มีนาคม 2563
60	Baseline	10.74.29.52	IMED-APP02		6 มีนาคม 2563
61	Internal	10.74.29.128	DCCEDADMZ1	01.00 - 04.00	6 มีนาคม 2563
62	Internal	10.74.29.129	DCCEDADMZ2		6 มีนาคม 2563
63	Internal	10.121.0.16/23	DCCEDAFID1		6 มีนาคม 2563
64	Internal	10.121.0.17/23	DCCEDAFID2		6 มีนาคม 2563
65	Internal	10.121.0.19/23	DCCEDAISS1		6 มีนาคม 2563
66	Internal	10.121.0.20/23	DCCEDAISS2		6 มีนาคม 2563

No	Testing approach	IP	System	Execution time	Execution date
67	Internal	10.121.0.25/23	DCCEDAESB1		6 มีนาคม 2563
68	Internal	10.121.0.26/23	DCCEDAESB2		6 มีนาคม 2563
69	Baseline	10.74.29.128	DCCEDADMZ1		6 มีนาคม 2563
70	Baseline	10.74.29.22	Flight Interface		6 มีนาคม 2563
71	External	110.170.118.64	adportal.airportthai.co.th.	17.00 - 23.59	5 มีนาคม 2563
72	External	110.170.118.65	elearning.airportthai.co.th.		5 มีนาคม 2563
73	External	110.170.118.61	portal.airportthai.co.th.		5 มีนาคม 2563
74	External	125.24.208.27	edoc.airportthai.co.th.		5 มีนาคม 2563
75	External	110.170.118.67	aoportal.airportthai.co.th.	01.00 - 02.00	6 มีนาคม 2563
76	Internal	10.74.29.240	CSM-APP	09.00 -12.00	7 มีนาคม 2563
77	Internal	10.74.29.241	CSM-DB		7 มีนาคม 2563
78	Internal	10.74.29.242	CSM-SERVICE		7 มีนาคม 2563
79	Internal	10.240.194.120	BI-APP		7 มีนาคม 2563

1.3. รายละเอียดวิธีการดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบ (Assessment Details)

ตารางด้านล่างแสดงถึงรายละเอียดวิธีการดำเนินการตรวจสอบช่องโหว่และทดสอบเจาะระบบ

Assessment Type	Description
การตรวจสอบช่องโหว่ (Vulnerability Assessment) จากเครือข่ายภายนอก (External Network)	บริษัทได้ดำเนินการตรวจสอบระบบเครือข่ายภายในและภายนอกของ ทอท. รวมถึง website ต่างๆ ที่ได้เปิดใช้งานสาธารณะ ตามขอบเขตของงาน การดำเนินการเป็นแบบ black box ซึ่งหมายถึงว่า ไม่ได้มีการส่งมอบข้อมูลอื่นๆ (เช่น username password หรือ ข้อมูลอื่นๆของระบบเป้าหมาย) นอกเหนือจาก IP address ของเครื่องเป้าหมายให้กับทางบริษัทใช้ในการ

Assessment Type	Description
	ตรวจสอบ การตรวจสอบใช้การอ้างอิงตามมาตรฐานสากล (OWASP Top 10) เพื่อระบุช่องโหว่และความเสี่ยงต่างๆ ของระบบ และแบบ Gray box คือได้รับทราบข้อมูลภายในบางส่วน เช่น network diagram การตั้งค่าความปลอดภัยภายใน และมีการปรับตั้งค่าการป้องกันของ firewall เพื่ออำนวยความสะดวกในการทดสอบ
การตรวจสอบช่องโหว่ (Vulnerability Assessment) จากเครือข่ายภายใน (Internal Network)	ในการตรวจสอบระบบภายใน ของทอท. บริษัทได้ดำเนินการที่ตึกสำนักงานการท่าอากาศยาน สนามบินสุวรรณภูมิโดยเชื่อมต่อเข้ากับเครือข่ายภายในของทอท. บริษัทได้รับมอบ IP Address จากทาง ทอท. เพื่อใช้ในการทดสอบ แบ่งเป็น Default Gateway IP 10.74.16.161 Static IP 10.74.16.164 สำหรับ Black box testing และ 10.74.16.165 สำหรับ Gray box testing
การทดสอบเจาะระบบ (Penetration Testing) จากเครือข่ายภายนอก (External Network) แบบ black box	บริษัทได้ดำเนินการทดสอบเจาะระบบเครือข่ายภายนอกของ ทอท. รวมถึง website ต่างๆ ที่ได้เปิดใช้งานสาธารณะ ตามขอบเขตของงาน การดำเนินการเป็นแบบ black box ซึ่งหมายถึงว่า ไม่ได้มีการส่งมอบข้อมูลอื่นๆ (เช่น username password หรือ ข้อมูลอื่นๆของระบบเป้าหมาย) นอกเหนือจาก IP address ของเครื่องเป้าหมายให้กับทางบริษัทใช้ในการตรวจสอบ การตรวจสอบใช้การอ้างอิงตามมาตรฐานสากล (OWASP Top 10) เพื่อระบุช่องโหว่และความเสี่ยงต่างๆ ของระบบ
การทดสอบเจาะระบบ (Penetration Testing) จากเครือข่ายภายนอก (External Network) แบบ Gray box	บริษัทได้ดำเนินการทดสอบเจาะระบบเครือข่ายภายนอกของ ทอท. ในแบบ Gray box คือได้รับทราบข้อมูลภายในบางส่วน เช่น network diagram การตั้งค่าความปลอดภัยภายใน และมีการปรับตั้งค่าการป้องกันของ firewall เพื่ออำนวยความสะดวกในการทดสอบ
การทดสอบเจาะระบบ (Penetration Testing)	ในการทดสอบระบบภายใน ของทอท. บริษัทได้ดำเนินการที่ตึกสำนักงานการท่าอากาศยาน สนามบินสุวรรณภูมิโดยเชื่อมต่อเข้ากับเครือข่ายภายในของ

Assessment Type	Description
จากเครือข่ายภายใน (Internal Network) แบบ black box	ทอท. บริษัทได้รับมอบ IP Address จากทาง ทอท. เพื่อใช้ในการทดสอบ แบ่งเป็น Default Gateway IP 10.74.16.161 Static IP 10.74.16.164 สำหรับ Black box testing
การทดสอบเจาะระบบ (Penetration Testing) จากเครือข่ายภายใน (Internal Network) แบบ Gray box	ในการทดสอบระบบภายใน ของทอท. บริษัทได้ดำเนินการที่ตึกสำนักงานการท่าอากาศยาน สนามบินสุวรรณภูมิโดยเชื่อมต่อเข้ากับเครือข่ายภายในของ ทอท. บริษัทได้รับมอบ IP Address จากทาง ทอท. เพื่อใช้ในการทดสอบ แบ่งเป็น Default Gateway IP 10.74.16.161 Static IP 10.74.16.165 สำหรับ Gray box testing
การตรวจสอบการตั้งค่ามาตรฐานความปลอดภัย (Security Configuration Baseline Assessment) ของเครื่องแม่ข่าย	บริษัทได้ดำเนินการตรวจสอบการตั้งค่าความปลอดภัยมาตรฐานของทอท. ที่ตึกสำนักงานการท่าอากาศยาน สนามบินสุวรรณภูมิโดยเชื่อมต่อเข้ากับเครือข่ายภายในของ ทอท. บริษัทได้รับมอบ IP Address จากทาง ทอท. เพื่อใช้ในการทดสอบ แบ่งเป็น Default Gateway IP 10.74.16.161 Static IP 10.74.16.164 และ 10.74.16.165

1.4. กฎการดำเนินการ (Rules of Engagement)

บริษัทฯ จะทำการทดสอบตามขอบเขตที่ได้กำหนดไว้ที่ระบบเครือข่ายและทำงานร่วมกับบุคลากรท่าอากาศยานไทย จำกัด (มหาชน) เพื่อจะเก็บข้อมูลและทดสอบจากระบบภายในองค์กรและวิเคราะห์ช่องโหว่ ขณะทำการทดสอบเจาะระบบอาจส่งผลกระทบกับระบบหรือบริการ โดยผู้ทดสอบจะหลีกเลี่ยงการทดสอบใดๆ ที่ส่งผลต่อระบบจนไม่สามารถให้บริการได้ ในกรณีที่ตรวจพบว่าช่องโหว่ดังกล่าวเป็นช่องโหว่ที่ทำให้เกิดผลกระทบอย่างรุนแรงมาก ทางบริษัทฯ จะไม่ทำการทดสอบนั้น เพื่อไม่ให้เกิดผลกระทบอันร้ายแรงจนไม่สามารถควบคุมผลกระทบที่อาจเกิดขึ้นได้ โดยมีรายละเอียด ดังต่อไปนี้

- การเปลี่ยนแปลงหน้าเว็บไซต์ (Defacement)
- การทำให้ระบบหยุดให้บริการ (Denial of Service) หรือการทดสอบใดๆ ที่ทำให้ระบบไม่สามารถให้บริการได้

- การเดารหัสผ่านด้วยจำนวน connection มหาศาล
- การทดสอบระบบใดๆ ที่นอกเหนือไปจากขอบเขตเป้าหมายในการทดสอบ

1.5. ข้อจำกัดของการประเมินความปลอดภัย (Limitation of Security Assessment)

ผลการวิเคราะห์ช่องโหว่ในรายฉบับนี้ มุ่งเป้าไปที่ช่องโหว่ของการรักษาข้อมูลและความลับของท่าอากาศยานไทย จำกัด (มหาชน) โดยรายงานฉบับนี้เป็นการทดสอบตามช่วงเวลาการทดสอบที่ได้ระบุไว้ ดังนั้นมีความเป็นไปได้ที่ระบบอาจมีการเปลี่ยนแปลงหลังการทดสอบ เช่น มีการแก้ไข ปรับปรุงระบบ เปลี่ยนแปลงระบบโดย ทอท. คำแนะนำและบทสรุป เพื่อทำการแก้ไขหรือปรับปรุงระบบจะมุ่งไปที่การโจมตีใดๆ ที่อาจเกิดขึ้นได้ การแก้ไขจุดอ่อนดังกล่าว ควรวิเคราะห์จากความรุนแรง ช่วงระยะเวลาและการส่งผลกระทบต่อระบบหลังการแก้ไข โดยหากไม่สามารถแก้ไขหรือการแก้ไขนั้นๆ ส่งผลกระทบต่อการใช้งานระบบโดยรวม แนะนำให้ใช้แผนหลีกเลี่ยงความเสี่ยงแทนรวมถึงการวางระบบตรวจจับการโจมตี ในระบบที่เป็นเป้าหมายแทน เพื่อให้ง่ายต่อการตรวจจับการโจมตีที่อาจเกิดขึ้นได้ รวมถึงหากเกิดเหตุการณ์โจมตีเกิดขึ้นในอนาคตก็พร้อมจะวิเคราะห์และแก้ไขได้ทันท่วงที

1.6. การสนับสนุน (Support provided)

บริษัทฯ ได้รับการสนับสนุนจาก ทอท. ดังต่อไปนี้

- ที่ทำงานและโต๊ะทำงานในสำนักงานของ ทอท.
- การเชื่อมต่อ Ethernet เข้าถึงเครือข่ายภายในของ ทอท.
- ข้อมูลเครือข่ายที่อยู่ IP ของเครือข่ายภายนอกและภายใน

1.7. ช่วงเวลาในการการทดสอบ (Project Timeline)

ตารางด้านล่างนี้ จะเป็นช่วงเวลาในการทดสอบ

Start Date	End Date	Phase	Location
2 มีนาคม 2563	7 มีนาคม 2563	● เครือข่ายภายใน (Internal Network) (Vulnerability Assessment and Penetration Testing) ● การตรวจสอบการตั้งค่ามาตรฐานความปลอดภัย (Security Configuration Baseline Assessment) ของเครื่องแม่ข่าย	ทอท. ท่าอากาศยานสุวรรณภูมิ
2 มีนาคม 2563	6 มีนาคม 2563	● เครือข่ายภายนอก (External Network) (Vulnerability Assessment and Penetration Testing)	Remote

1.8. รูปแบบการจัดอันดับความเสี่ยง (Severity Ranking Model)

การจัดอันดับความเสี่ยง ทางบริษัทได้ใช้รูปแบบตามมาตรฐานสากลอ้างอิงตาม Common Vulnerability Scoring System version 3 (CVSSv3) ซึ่งสามารถอ้างอิงได้จาก

https://www.first.org/cvss/v3.0/specification-document

Severity		CVSS 3 Score	Description
C	Critical	9.0 - 10.0	เป็นช่องโหว่ที่จำเป็นต้องแก้ไขทันที ช่องโหว่ดังกล่าวทำให้ผู้โจมตีสามารถเข้าถึงระบบได้ หรือทำให้สามารถเข้าถึงข้อมูลสำคัญ ได้ เช่น ข้อมูลทางการเงินหรือการกระทำที่ทำให้เกิดความเสียหายต่อชื่อเสียง เป็นต้น
H	High	7.0 - 8.9	เป็นช่องโหว่ที่ทำให้ข้อมูลรั่วไหลหรือถูกแก้ไขได้และเป็นช่องโหว่ ที่ทำให้ผู้โจมตีสามารถมีสิทธิ์เข้าถึง networks, systems, หรือ applications อื่นๆ ได้
M	Medium	4.0 - 6.9	เป็นช่องโหว่ที่จะนำไปสู่การยึดเครื่องแต่อาจต้องใช้ปัจจัยอื่นๆ เพื่อทำให้การโจมตีสำเร็จ เช่น จำเป็นต้องใช้การโจมตีอื่นๆ ประกอบด้วย เพื่อให้เกิดผลกระทบการเข้าถึงอย่างมีขีดจำกัด

Severity		CVSS 3 Score	Description
			จำเป็นต้องใช้ความรู้ขั้นสูงและเทคนิคขั้นสูงในการโจมตี เป็นต้น
L	Low	0.1 - 3.9	เป็นช่องโหว่ที่ไม่สามารถเอามาใช้งานได้โดยตรง จำเป็นต้องมีการใช้งานช่องโหว่หลายช่องโหว่ร่วมกันหรือเป็นช่องที่ทำให้ข้อมูลไม่สำคัญหลุดออกมาหรือเป็นช่องโหว่ที่ไม่ได้นำไปสู่การยึดเครื่องเป้าหมาย