HIPAA Compliance Report

from 2009-09-17 16:18:33 to 2009-09-18 16:18:33

System Name: AirDefense
Domain: System
Generated: 2009-09-18 16:19:42
Version: 7.3.3-12
Time Zone: EDT - Eastern Daylight Time

HIPAA Requirement Summary

The HIPAA Security Rule requires that Protected Health Information (PHI) that is transmitted over public networks be encrypted by a commercially acceptable encryption mechanism. Because the very nature of wireless LANs requires that they broadcast data in the air, they should be considered public networks and must meet the encryption requirement to maintain HIPAA compliance per Section 164.312(e)(1) of the HIPAA Security Rule 45 CFR Subpart C.

This report details the policies of this institution regarding encryption requirements for each wireless access point. It also indicates where violations may occur: due to mis-configurations of access points, deployments of improperly configured unauthorized or "rogue" access points, user stations roaming to unsecure neighboring networks without the user's knowledge and other scenarios that would undermine the required encryption policy.

This report is based on real-time monitoring of the airwaves throughout this institution and includes all violations to policy as well as how timely a response is given to policy violations per Section 164.308(a)(6). Because monitoring is done constantly, this report also reflects the discovery and vulnerability assessment requirements of the HIPAA rule in regards to maintaining a security management process per Section 164.308(a)(1).

Policy Compliance Summary

APs without Proper Authentication:	7
APs without Proper Encryption:	5
Rogue Access Points:	110
Rogue Stations:	15
Unauthorized Roaming between APs:	0
After-Hours Activity:	0
Severe and Critical Alarm Count:	466
Severe and Critical Uncleared Alarms:	466

Specific Policy Violations (Up to 50 Listed)

Total Policy Violations	19

Device	Device MAC	Sub-Category	Alarm	Start Time	Location	Group	Cleared
Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Advanced Key Generation	Advanced Key Generation Modes Violated	8/11/09 6:49 PM	Auburn, GA	Auburn	No
Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Authentication	Extended Authentication Modes Violated	8/11/09 6:49 PM	Auburn, GA	Auburn	No
Belkin:c2:ff:c3[b,g]	00:1c:df:c2:ff:c3	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/11/09 6:50 PM	Auburn, GA	Auburn	No
Symbol:4f:e4:1c[a,b,g]	00:15:70:4f:e4:1c	Authentication	Extended Authentication Modes Violated	8/5/09 5:05 PM	Atlanta, GA Office	1st Floor	No
Symbol:50:1f:40[a,g]	00:15:70:50:1f:40	Authentication	Extended Authentication Modes Violated	8/5/09 5:02 PM	Atlanta, GA Office	1st Floor	No

Device	Device MAC	Sub-Category	Alarm	Start Time	Location	Group	Cleared
Symbol:4f:de:64[a,g]	00:15:70:4f:de:64	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
Symbol:50:1e:54[a,b,g]	00:15:70:50:1e:54	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
Symbol:4f:e4:80[a,b,g]	00:15:70:4f:e4:80	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	802.11 Encryption	80211 Encryption Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	Authentication	Extended Authentication Modes Violated	8/5/09 5:01 PM	Atlanta, GA Office	1st Floor	No
Nortel:76:7d:40[a,b,g]	00:18:b0:76:7d:40	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	8/5/09 5:02 PM	Atlanta, GA Office	1st Floor	No
Symbol:27:e1:b0[a]	00:15:70:27:e1:b0	Incorrect AP Configuration Observed	AP SSID Broadcast in Beacon	9/11/09 1:55 PM	Atlanta, GA Office	1st Floor	No
Symbol:50:1f:40[a,g]	00:15:70:50:1f:40	802.11 Encryption	80211 Encryption Modes Violated	9/14/09 8:47 AM	Atlanta, GA Office	1st Floor	No
Symbol:50:1e:54[a,b,g]	00:15:70:50:1e:54	802.11 Encryption	80211 Encryption Modes Violated	9/14/09 9:48 AM	Atlanta, GA Office	1st Floor	No
Symbol:4f:e4:80[a,b,g]	00:15:70:4f:e4:80	802.11 Encryption	80211 Encryption Modes Violated	9/15/09 8:09 AM	Atlanta, GA Office	1st Floor	No
Askey:05:6f:39[a,b,g]	00:11:f5:05:6f:39	Environment	Ad-Hoc Network Violation Unauthorized Device	9/17/09 11:26 AM	Atlanta, GA Office	1st Floor	No
Symbol:27:e1:b0[a]	00:15:70:27:e1:b0	802.11 Encryption	80211 Encryption Modes Violated	9/17/09 5:13 PM	Atlanta, GA Office	1st Floor	No
Liteon:b0:82:2d[b]	00:22:5f:b0:82:2d	Environment	Ad-Hoc Network Violation Unauthorized Device	undefined time	Atlanta, GA Office	1st Floor	No
Liteon:b0:82:2d[b]	00:22:5f:b0:82:2d	Environment	Ad-Hoc Network Violation Unauthorized Device	9/18/09 11:46 AM	Atlanta, GA Office	1st Floor	No