Priavo 360 Maritime Security

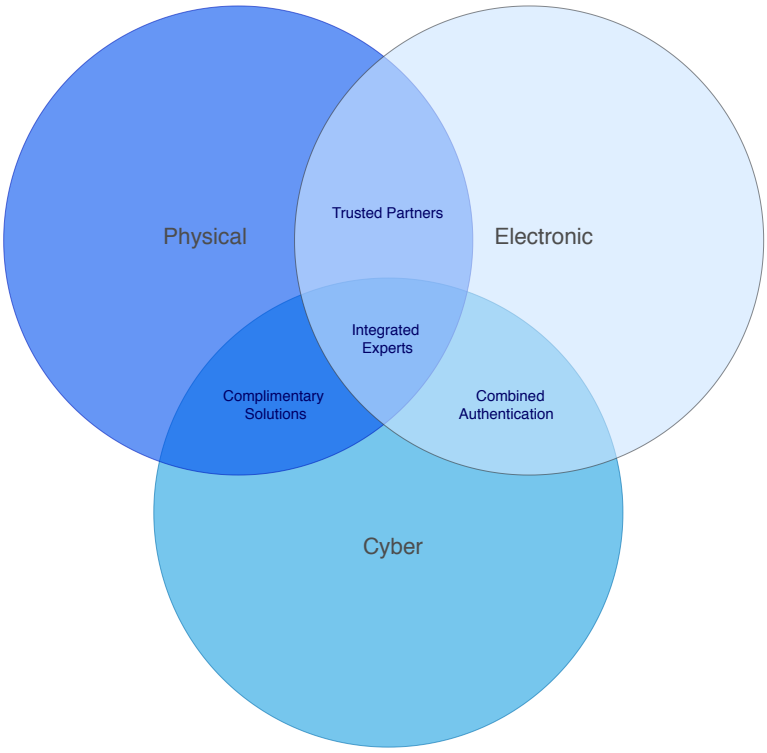
Monaco Yacht Show Cyber Review

October 2019

Priavo Maritime Security
| 84 Brooke Street | Mayfair | London | W1K 5EH |
Email: enquiries@priavosecurity.com | Visit: www.priavosecurity.com.com

Priavo Maritime Security 360 Alliance

Priavo Security is a leading Security and Risk Management Company with project experience globally.
Our Maritime 360 Alliance was created to provide a multi-layered protective service to combat evolving attacks and our team have gained maximum exposure to the sophisticated security threats facing the industry today. 360 brings an amalgamation of three established industry leaders across physical, electronic and Cyber security to provide an integrated and comprehensive security partnership. The projects success is due to the ability to work seamlessly together, considering the unique safety and privacy requirements of each client.



Physical Security

We have a multi-disciplinary team of field-based security operatives comprising of experience from UK Special Forces, Military, Police and Intelligence agencies.

Electronic Security

Technology is constantly advancing. A security system needs to automatically detect, track, classify and alert client's to activity in the vicinity.

Cyber Security

We focus on the protection, detection and incident response for all cyber security threats through cyber threat intelligence and 24/7 managed services.

Wi-Fi Security at Monaco Yacht Show Overview

Cyber Infrastructure Review

Our 360 Maritime Security team attended the 2019 Monaco Yacht Show last month and conducted cyber testing. Basic passive tests were conducted to gain a high-level view of the quality of WI-FI security controls implemented on yachts, as well as a review of the security at the show itself.

Whilst wireless is only a small component of a yachts security, it can be visible to people nearby. Potential attackers will be attracted to vessels that appear 'less secured' than others. The team did not carry out any intrusive or in-depth testing as they would usually do under a formal penetration testing engagement, however by passively monitoring the airwaves they were able to gain information about the security controls on-board.

Owners, Captains, Crew and Management were invited to our live hacking demonstration on Friday and Saturday of MYS2019, which demonstrated how quickly we could gain complete uncontrolled access to multiple types of wireless, control and CCTV networks on various yachts.

Cyber Infrastructure Review Continued

Using practical examples our Cyber team explained the best methods for reviewing and securing existing networks on-board, demonstrating the ease of use and immediate benefit of our decoy and deception system.

By luring attackers to connect to a fake deception system, it acts as an early warning system of a cyber-attack. Technology improvements can often take several months to implement on a vessel due to the approval and testing process. A deception system gets around this delay because there are no changes to the existing systems whilst giving you an immediate level of visibility and an indication of a positive breach.

The tests were split into 2 sections:

1. A review of the WI-FI and visible security systems protecting owners, crew and guests, and automation designed to highlight whether there are any obvious flaws that would allow unauthorised access.
2. Deployment of a fake deception system on the show WI-FI, with enhanced monitoring of security activity. Designed to highlight if anyone is running security reconnaissance and attempting to hack systems at the show.

The team conducted passive scans of the airwaves: no active scans were conducted that would have required approval. However, it does beg the question: would anyone have noticed? The only time the team were challenged during the demonstration period was when we openly walked around the show with a device that looked like a TV antenna (see image below).

Unattended laptop performing WIFI hacking during the London Olympics

Security scanning and assessments were performed covertly from a device the size of a mobile phone hidden in a pocket. It would be expected that on-board cyber monitoring would pick up suspicious behavior, not just identify a threat when a 2-foot antenna is pointed towards a vessel.

Previously our team was contracted by the City of London, MOD and GCHQ to perform penetration tests at the London Olympics. Again unattended and unchallenged, a 'hacking laptop' was placed in full view, blatantly evaluating the security of the yachts and WIFI in Canary Wharf.

Privacy impact: The goal behind the analysis was to gain a quick view of the general protection levels on ships in the area and their typical security posture. The test team did not specifically target any specific vessel or include any specific data or screenshots as they contained information that may lead to the identification of vessel, onboard systems and crew or owner.

Cyber Expert performing passive cyber testing of yacht systems at MYS 2019

Phase 1 Findings:

All wireless networks were profiled and were grouped based on common vulnerabilities and protection methods to highlight similarities in multiple systems across vessels:

- **675 distinct wireless networks were identified at the show**, these included show WI-FI, yacht internet and control systems and personal hotspots.
- Of the 675 wireless networks identified, **17 were found to be 'secured'** and using individual user authentication to connect to the WI-FI network itself. All others had some level of vulnerability or configuration that is not considered 'secure' and not in line with security guidelines from IMO, Bimco. Please see graphic on WI-FI standards below.
- **58 wireless networks were related to internal control systems that should not be visible to the general public.** Automation systems such as Crestron, Control4 and Savante, along with OT and operational systems, access control and CCTV all had wireless connectivity. These were visible to anyone passing by who could attempt to authenticate: these systems should either have no wireless access or have strong authentication and control.
- **11 networks were found to be using an old encryption system** (WEP) that was compromised at least 10 years ago and is prohibited for use in any wireless network. It can be hacked within minutes.

- **25 networks were named YACHTNAME-OWNER or YACHTNAME-O**, this is obviously a strategy to separate the principal's devices from the rest of the crew. However, this also shows anyone watching which devices connect to the 'owners' network and marks them as more of a target. It is recommended to either name the owner network as a non-descript name or, preferably to use a single network name and provide the segmentation through strong authentication and firewall control rather than basic name separation of wireless networks.
- **89 open networks were identified that had no encryption upon connection** and also enforced no authentication. Some of these networks did attempt to authenticate users once they had connected but this has a major flaw for all but untrusted guest networks. If an attacker pretends to be the same network name as the open one, any devices which has connected to it previously will inadvertently connect to the fake network automatically, passing all traffic via an unauthorized third party.
- **564 (the remainder) have encryption enabled but share a single password** (WPA key) amongst all users. This method is flawed for secure networks, not only for the fact that a single password only needs to be lost once before giving someone access but also, an attacker can easily see a scrambled version (hash) of a user login session. This 'hash' can then be taken away and compared against a dictionary of password combinations and can reveal the true password. This method was demonstrated at the event with 6 accounts relating to both crew, owner and officer network devices.

Monaco: Port Hercules

Phase 2 Findings:

Deception systems were connected to the MYS Wi-Fi system. These decoys appear to be normal computers but openly broadcast the fact that they are easy to compromise. Any attacker once connected to a target network will look for a system that appears to be vulnerable and will likely attack that before others. Monitors were put in place to identify and alert on this suspicious activity:

- 2 other devices were identified as making active probes in the airspace of the MYS environment. Both devices were monitored attempting to connect to multiple vessels networks and exhibiting behavior that is only used in the early stages of attack. It is not known if this activity was targeted or opportunistic, or if someone was just 'playing' with some hacking tools. In our experience there are often attempts to connect to unauthorized networks but then again, MYS is a prime location and a good time to survey a potential target vessel system in a crowded environment where they are unlikely to be caught.

- The MYS show Wi-Fi was actually one of the better secured systems. The show Wi-Fi does not have any sensitive data to protect and only needs to separate exhibitors and guests yet they have implemented individual user authentication at the wireless access point level and some level of protection between users. We did notice at least two people attacking the MYS Wi-Fi system and would recommend that the show does improve monitoring and protection against future Wi-Fi attacks. We have offered to provide a FOC protection service for next years show.

In Layman's Terms:

Use individual usernames and passwords for each user to logon, no shared, single password. Monitor the air (as we have done) to spot hackers trying gain access via wireless technology.

Last Word of Caution:

Do not think you are safe when you cannot see the threat. There is a tendency to feel there is no threat to electronic systems when at sea. This is not the case. Sat-com and personal devices all have connectivity, long range wireless antenna can connect to a ship from a distance and are inexpensive. In addition, there are also wireless and other radio-based attacks from the air and more recently from underwater. Even when disabled, AIS means that people know roughly where the crew and Principal are most of the time. This is unique and is becoming an increasingly popular time to target people, assets and data.

Recommendations:

Conduct a whole ship threat assessment, evaluate all ship systems as a single platform and protect the weakest link. A cyber review is a single element of evaluating the security of a Super-yacht, both physical and electronic security require due consideration. Attackers are using multiple vectors to compromise systems and protection frameworks must cover all avenues of potential compromise. A vessel that doesn't take basic precautions certainly won't have any in depth security layers to protect owners and crew. 360 Maritime Security can develop plans for a ship, owner and crew to be fully compliant with the IMO security standards and can offer an integrated protection service covering physical, cyber and electronic controls.