SECURING IT SYSTEMS FOR A LEADING MARITIME TECH COMPANY

In recent years, the maritime industry has become highly concerned about cybersecurity. As yachts become more reliant on tech, they become more vulnerable to attacks. The consequences of a security breach could be disastrous, including:

- Compromising of data
- Disruption to critical IT systems
- Potential impact on safety

For a market-leading tech business specialising in designing IT systems aboard vessels, ensuring these systems are safe and secure is a top priority.

Discovery

While each vessel is slightly different, we compiled a general overview of IT infrastructure aboard a vessel. Of the many aspects we talked about, here are three key findings:

- Ships can contain the same amount of switches and access points you might encounter in a medium-sized organisational infrastructure. Much like desktops, laptops, phones and systems are connected to these switches and access points.
- Even more access points may be needed onboard a superyacht. Wi-Fi connection can be erratic due to the amount of steel used to build a ship.
- Network segmentation, similar to a typical modern-day infrastructure is required in this environment as well.

Challenges

After the initial call, we were able to clarify with our client the most pressing IT security challenges they face, and their causes. The most pressing concern for our clients was that the Wi-Fi's Network Access Control (NAC) needed to be simplified. The onboard AV/IT personnel needed an easier solution for network access control. Our client was losing more time than necessary with remote supporting Wi-Fi access.

Their aim is to move away from manually setting up switch ports. Currently, access ports on the switches are manually assigned to a VLAN. So, if anyone ever needed to move a desktop computer, laptop or phone, they needed to request support. Of course, manually setting up switch ports is time-consuming and can lead to errors.

Problem-solving

At Soliton, we're all about helping businesses discover ways to keep their IT systems more secure. That's why we developed the Clear Path Forward (CPF) report. After a conversation where our experts will help clarify IT security challenges, we'll produce a comprehensive report recommending the optimal solution and proposing a business case to get the project moving.

It was clear that we could solve both of these challenges by implementing a dedicated Network Access Control solution for both the Wi-Fi and cabled access ports. This NAC system would need to be:

- Easy to implement and manage
- Resistant to failure with high availability
- Stripped of all frills to boost efficiency

The solution

Based on these requirements, we recommended the Soliton NetAttest EPS solution in our Clear Path Forward report.

NetAttest EPS solution is self-contained and removes the dependency on Microsoft NPS and the Active Directory Certificate Services. To boost availability, one NetAttest EPS will be connected to the first core switch and the other to the second, then both will be back-to-back connected for high availability.

Configuration is simple. The next step is configuring the access switches and Wi-Fi access points so they can use both NetAttest EPS RADIUS servers for port authentication. Once configured, it can specify per access port whether 802.1X port authentication should be used, similar to Wi-Fi SSIDs.

Soliton KeyManager also makes it possible to install certificates on BYOD devices. The device does not have to be domain joined or managed to do this. When guests are only staying for a short time, the client can issue a temporary access code so that they can use the guest Wi-Fi. Guests will use a customisable portal page to access. Other benefits of the NetAttest EPS product line include:

- Fast setup through the setup wizard,
- Create full backup
- Restore in minutes

Future-proofing

While it's essential to fix the problems clients face today, it's even better if you can help safeguard them for the future too. During the sessions with the client they shared their product development strategy , which meant we could accommodate this in the solution recommendations.

Justifying the investment

It is important to justify the cost and benefits of an upgraded IT security solution to internal stakeholders. After sharing the Clear Path Forward report, we agreed to work with the client to build a business case for investment in IT security.

Discover your Clear Path Forward

At Soliton, we've delivered innovative IT security solutions to large and small businesses for over 40 years. We created the Clear Path Forward Report to help businesses like yours better understand their IT security and design the best solutions.

Here's how it works. IT departments that want to explore their options can arrange your workshop with a Soliton expert adviser, who will:

- Dive deep into your existing IT security setup
- Identify risks and their impact on your business
- Discover the real problems behind your cybersecurity headaches

Soon after your workshop, we'll deliver your Clear Path Forward report. This comprehensive, plain-speaking report sums up the challenges you're facing right now - and recommends solutions.

The report is a 2-3 page structured business case for investment in cybersecurity, which you can use to bring in the other stakeholders in your company and get the project moving.

Once you know your problems and how they truly affect your business, you can start doing something about them. Discover more about the Clear Path Forward Report here.