* Investigate the various security concerns this company has had, and might have in the future

Shell like many other companies big and small fell victim to an attack however this kind of attack exploited an old piece of equipment. (Forbes, 2021) This allowed attackers to steal sensitive information not only from Shell but “some of their stakeholders”.

The company equipment is also running an older operating system called CentOS 6 which is also end of life (CentOS Wiki, 2021) and with an operating system not receiving any new security updates or patches will result in them being vulnerable going forward.

References

<https://www.forbes.com/sites/leemathews/2021/03/23/oil-giant-shell-victimized-in-december-2020-hack/?sh=6c8f8b9114f2>

<https://wiki.centos.org/About/Product>

* Provide exemplars of how these concerns have been or can be dealt with by the company. How have other multi-national organizations mitigated such issues?

Shell worked with the vendor (Forbes, 2021) and the equipment was “isolated from the rest of Shell’s network”. This means that even if attackers got through again, they would not be able to traverse the network and steal more data.

According to Forbes, about 50 other companies were still using the old equipment of which a large number of them had data losses.

According to CPO Magazine (March 2021) one of the other victims “Kroger” were also part of the same attack.

Other vulnerabilities were found but addressed quickly and as per Accellion did not yield any cyber-attacks.

References

<https://www.accellion.com/company/security-updates/mandiant-issues-final-report-regarding-accellion-fta-attack/>

<https://www.cpomagazine.com/cyber-security/accellion-cyber-attacks-explode-as-criminals-exploit-multiple-fta-vulnerabilities/>

<https://www.accellion.com/company/security-updates/mandiant-issues-final-report-regarding-accellion-fta-attack/>

* Based on this example, what issues do you foresee as a Cyber Security professional if employed by multinational companies? How does this compare with issues faced by small and medium-sized companies?

If we chat about small and medium sized companies, they do not always have the budget to employ a full cyber security professional or a team to look at the security all the time and rely on 1 or 2 IT staff members to carry everything.

For a large corporate, they may be able to employ a team of experts to address issues. The main issue I can see that is if companies are running legacy hardware and software running systems may still be at risk for continuous Cyber-attacks or have back doors where data is constantly being stolen before being exposed to the highest bidder on the dark web.