



Medical Mannequin: Initial Post

Course: MSc Computer Science

Module: Network and Information Security Management

Assignment: ePortfolio

Date: Wednesday 22nd September 2021

Student ID: 126853

Post:

A 2017 research paper (Martin, G. et al., 2017) states that there has been a 300% increase in cyberattacks directed towards the healthcare sector in 3 years, with only half of providers believing they could mitigate an attempted attack. One example of an attack on the healthcare sector was on Friday 12th May 2017, where the NHS was targeted by a ransomware virus nicknamed 'WannaCry' (Acronis, n.d.).


Although this attack didn't prove to be catastrophic, it did cause significant disruption to the daily tasks staff were required to complete, with some reports stating that staff had resorted to pen and paper for data recording.

Glisson et al. (2015) explored the potential vulnerabilities in the healthcare sector, demonstrating an attack on a training mannequin provided by the College of Nursing at the University of South Alabama. Students managed to identify a series of vulnerabilities, including WiFi password brute-forcing and a denial of service attack using a WiFi de-authentication attack, which caused the training host PC to lose connection to the mannequin. Both vulnerabilities would have allowed an attacker to disrupt a session or potentially trigger incorrect scenarios on the device.

In the above cases, a series of minor amendments could be made to protect these vulnerabilities, including using a wired connection (or wireless with whitelisting and a complex password) and updating to the 802.11W (2009) standard, which provides management frame protection (Making deauth attacks more difficult to achieve).

One of the first stages of mitigating attacks is to ensure that all software is kept up-to-date (Kruse et al., 2016), with patches being applied soon after release/vulnerability disclosure. IT Administrators should also ensure that staff members are provided with the minimum level of system access to perform their roles (Coronado & Wong, 2014). All healthcare providers should also consider hiring penetration testers to perform audits on their technology and provide regular training to all staff members to identify and prevent potentially malicious actions.

Screenshot:


Kieron Holmes

Initial Post
37 days ago

2 replies
Last 32 days ago

A 2017 research paper (Martin, G. et al., 2017) states that there has been a 300% increase in cyberattacks directed towards the healthcare sector in 3 years, with only half of providers believing they could mitigate an attempted attack. One example of an attack on the healthcare sector was on Friday 12th May 2017, where the NHS was targeted by a ransomware virus nicknamed 'WannaCry' (Acronis, n.d.). Although this attack didn't prove to be catastrophic, it did cause significant disruption to the daily tasks staff were required to complete, with some reports stating that staff had resorted to pen and paper for data recording.

Glisson et al. (2015) explored the potential vulnerabilities in the healthcare sector, demonstrating an attack on a training mannequin provided by the College of Nursing at the University of South Alabama. Students managed to identify a series of vulnerabilities, including WiFi password brute-forcing and a denial of service attack using a WiFi de-authentication attack, which caused the training host PC to lose connection to the mannequin. Both vulnerabilities would have allowed an attacker to disrupt a session or potentially trigger incorrect scenarios on the device.

In the above cases, a series of minor amendments could be made to protect these vulnerabilities, including using a wired connection (or wireless with whitelisting and a complex password) and updating to the 802.11W (2009) standard, which provides management frame protection (Making deauth attacks more difficult to achieve).

One of the first stages of mitigating attacks is to ensure that all software is kept up-to-date (Kruse et al., 2016), with patches being applied soon after release/vulnerability disclosure. IT Administrators should also ensure that staff members are provided with the minimum level of system access to perform their roles (Coronado & Wong, 2014). All healthcare providers should also consider hiring penetration testers to perform audits on their technology and provide regular training to all staff members to identify and prevent potentially malicious actions.

References:

Martin, G. et al. (2017) Cybersecurity and healthcare: how safe are we? *BMJ* 358(j3179). DOI: <https://doi.org/10.1136/bmj.j3179> [Accessed 15th August 2021].

Acronis. (n.d.) The NHS cyber attack. Available From: <https://www.acronis.com/en-gb/articles/nhs-cyber-attack/> [Accessed 15th August 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. *Healthcare Information Systems and Technology (Sighealth)*. Available From: <https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf> [Accessed 15th August 2021].

Kruse, C., Frederick, B., Jacobson, J., Monticone, K. (2016) Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care* 25(1): 1-10. DOI: <https://doi.org/10.3233/thc-161263> [Accessed 15th August 2021].

Coronado, A., Wong, T. (2014) Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. *Biomed Instrum Technol* 48(s1): 26-30. DOI: <https://doi.org/10.2345/0899-8205-48.s1.26> [Accessed 15th August 2021].

References:

Acronis. (n.d.) The NHS cyber attack. Available From: <https://www.acronis.com/en-gb/articles/nhs-cyber-attack/> [Accessed 15th August 2021].

Coronado, A., Wong, T. (2014) Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomed Instrum Technol 48(s1): 26-30. DOI: <https://doi.org/10.2345/0899-8205-48.s1.26> [Accessed 15th August 2021].

Glisson, W., Andel, T., McDonald, T., Jacobs, M., Campbell, M. & Mayr, J. (2015) Compromising a Medical Mannequin. Healthcare Information Systems and Technology (Sighealth). Available From: <https://arxiv.org/ftp/arxiv/papers/1509/1509.00065.pdf> [Accessed 15th August 2021].

Kruse, C., Frederick, B., Jacobson., Monticone, K. (2016) Cybersecurity in healthcare: A systematic review of modern threats and trends. Technology and Health Care 25(1): 1-10. DOI: <https://doi.org/10.3233/thc-161263> [Accessed 15th August 2021].

Martin, G. et al. (2017) Cybersecurity and healthcare: how safe are we?. BMJ 358(j3179). DOI: <https://doi.org/10.1136/bmj.j3179> [Accessed 15th August 2021].