JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog November 2020

Topics covered in this issue:

- An implantable defibrillator patient describes his Cybersecurity concerns
- Malicious actors attack the Covid-19 vaccine supply chain

An implantable defibrillator patient describes his Cybersecurity concerns

https://onezero.medium.com/i-live-with-a-digital-security-threat-inside-my-body-ca6b9da0b316

The above article was written by Jameson Rich for medium.com in November of 2020, and provides an important, highly personal account of the author's experience with a severe health issue, a medical device, and the cybersecurity concerns and realities that a patient is subject to in these situations. It is rare to find patient-focused or patient-authored narratives which focus on medical device cybersecurity, and because of that there is the potential for professionals who are stakeholders in the field of medical device cybersecurity, at least those who aren't healthcare providers directly interacting with the patients involved, to perhaps minimize or overlook the individual, human dimensions involved in the modern medical device landscape. While cybersecurity is a paramount and ever-evolving consideration amongst all aspects of modern life, perhaps nowhere is the threat more acute and tangible then within the healthcare industry, and, more specifically, medical devices.

The article starts with the author, Mr. Rich, recounting a night in late December of 2016 where he began experiencing what was later diagnosed as ventricular tachycardia-where only one side of the heart pumps and does so rapidly. This resulted in a call to emergency services and two rounds of defibrillation, eventually leading to a hospital stay and months of testing. Mr. Rich states in the article that following his hospitalization, he underwent several months of testing and medication. Ultimately, his doctors suggested that his pacemaker, which he had already been utilizing following a lifetime of arrythmias, be replaced with what is known as an ICD (implanted cardioverter-defibrillators, which he describes in the article as " a fail-safe, a tiny defibrillator inside my body that could go wherever I went".

John Ward – Cyberblog November 2020

Prior to Mr. Rich's surgery to implant the device, he found an FDA safety notice issued on January 9th, 2017 that indicated that some ICD's, particularly those produced by a company known as St. Jude, were vulnerable to hacking by malicious external actors. The possibility would then exist that the malicious actors could inflict harm upon the individual who has been implanted with an ICD, up to and including death (this FDA safety notice, as well as subsequent FDA safety notices pertaining to St. Jude's-produced ICD's, were examined by this author in a previous resource list submitted to Ward Sciences and Consulting LLC).

This FDA safety notice clearly gave Mr. Rich some misgivings regarding the implantation of the ICD into his body and, as he relays in the article, he contacted his nurse practitioner regarding the matter. According to Mr. Rich, her response was that he need not be worried because the ICD that was being implanted in his body because his specific ICD would be produced by a company other than St. Jude. Mr. Rich eventually decided to go ahead with the procedure, but relayed that he constantly lives with the fear that one day, with no warning, he could be injured or called solely based on the whim of a remote hacker.

According to Mr. Rich, ICD's were initially introduced in the 1980's, and in the time since have proliferated rapidly in the medical device community. According to Mr. Rich, "…doctors currently implant at least 10,000" ICD's every month in the United States, and that the devices have become "fully integrated into the so-called Internet of Things". This topic has been discussed at length in previous resource lists and reports by this author to Ward Sciences and Consulting LLC, and as the Internet of Things grows more ubiquitous within every aspect of modern life, the greater the risk that these devices, whether mundane devices such as refrigerators or devices critical to health, such as ICD's, are able to be accessed (or at the very least have access by the appropriate user denied, such as in ransomware attacks) by malicious actors.

Mr. Rich's story highlights both positive and negative and the current medical device cybersecurity landscape, from an intimate, patient-focused point of view. Mr. Rich was able to quickly access important information regarding the current (at the time) state of ICD cybersecurity, an easily accessed and thorough government-released safety warning issued under the auspices of the FDA. In a democracy, such as the United States, the division between governmental oversight and private enterprise is a cornerstone-even in matters security, either national or personal, legislation is often required to compel private industry to adopt new regulations. This is a timely process, with an uncertain result.

John Ward – Cyberblog November 2020

Thus, the United States government, as discussed in previous reports and resource lists by this author for Ward Sciences and Consulting LLC, serves primarily as a resource for information and coordinator of stakeholders in regards to cybersecurity over all matters of critical infrastructure. The fact that Mr. Rich was able to locate information regarding the St. Jude safety notice on his own is an affirmation of this model of cybersecurity awareness. However, just being aware of a potential cybersecurity issue is only one component of a robust and effective cybersecurity policy. It is troubling, and indicative of the major deficiencies which can still exist within the patient-healthcare provider dynamic in regards to cybersecurity, that Mr. Rich located the information on his own accord, and was not informed of the cybersecurity concerns of having an ICD. Furthermore, his concerns were addressed in a cursory response which did not have any specifics beyond the fact that the brand used by his healthcare provider was not the same one identified in the FDA notice. It is important for patients in any healthcare procedure or environment to remember that they are their own best advocates, but in Mr. Rich's case the cybersecurity component of his implantation was entirely ignored, and if he did not take it upon himself to investigate himself than he may very well still be ignorant of the risks to this day-which raises the question of how many medical device implantation patients are living today without any idea of the risks that they have been exposed to?

This article is entirely anecdotal and does not reflect the experience of all patients who are implanted with medical devices, but it is an important reminder of the stakes involved with cybersecurity in medical devices. It is entirely possible that some healthcare providers are not as neglectful in informing the patient of the cybersecurity risks of a medical device, nor as dismissive of their inquiries, but Mr. Rich's article paints a troubling picture that the matter appears to be of little importance to his particular healthcare provider. Furthermore, this article highlights an important aspect of medical device cybersecurity as it pertains to patient health, and that is the patient's mental health. Thanks to the FDA's safety notice the potential (and potentially catastrophic) security flaws of the device, at least the model produced by St. Jude, are known by Mr. Rich and he is aware of the physical risks of being implanted with an ICD. But Mr. Rich ends the article by stating that he is "…stalked by…fear" in regards to the knowledge that his ICD, implanted within his body, could potentially be used against him. It is the opinion of this author that this would require a shift in healthcare providers' approaches to letting patients know the cybersecurity risks of devices implanted in them (or external devices used in their care), to a level of importance that they place on speaking with patients regarding potentially harmful effects of medications or surgeries.

SCIENCES AND CONSULTING

JOHN WARD CYBERSECURITY BLOGS

YOUR ONLINE RESOURCE FOR TIMELY ANALYSIS, COMMENTARY AND RESOURCES TO KEEP YOU INFORMED ON THE EVER EVOLVING AND HIGHLY CRITICAL FIELD OF CYBERSECURITY

John Ward – Cyberblog November 2020

Malicious actors attack the Covid-19 vaccine supply chain

https://us-cert.cisa.gov/ncas/current-activity/2020/12/03/ibm-releases-report-cyber-actors-targeting-covid-19-vaccine-supply

The second resource explored in this document explores a recent threat regarding malicious actors targeting the "cold-supply" chain of the COVID-19 vaccine, and an exploration of the many aspects of cybersecurity detection, notification, and coordination that are ideally involved with high-level cyber threats in the United States when they pertain to critical infrastructure.

The above-linked resource is a notification from the Cybersecurity & Infrastructure Security Agency (CISA), which is a federal agency under the oversight of the Department of Homeland Security. According to CISA's website, their role is to "…build the national capacity to defend against cyber attacks and work within the federal government to provide tools, incident response services, and assessment capabilities…". Essentially, CISA exists to serve as a primary source of research, information and tools in the ever-evolving world of cybersecurity and the battle against cyberthreats. Through an examination of recent, prescient events within the cybersecurity and healthcare communities, one can examine the fruitful collaboration of private enterprise and public resources and conclude that both have important roles to play.

According to the CERT release, IBM's X-Force, described by IBM as a "cloud-based threat intelligence platform that allows [the stakeholder] to consume, share, and act on threat intelligence". In this case, the IBM X-Force has identified that "malicious cyber actors [are] targeting the COVID-19 cold chain-an integral part of delivering and storing a vaccine at safe temperatures". It is impossible to over-emphasize the importance of a rapid supply chain for a COVID-19 vaccine, so much so that the official name of the process is "Operation Warp Speed". The IBM X-Force has found that malicious actors are not targeting the direct production of the vaccine, but instead are attacking integral parts of the supply chain through phishing and spearphishing emails in an effort to "harvest account credentials". CERT has taken these findings and issued a warning on their website as an addition to their National Cyber Awareness System, designed to serve as a one-stop shop for important, prescient cyber-threats affecting all areas of the critical infrastructure. CISA then augments the IBM X-Force's findings with it's own proprietary supplemental resources, such documents pertaining to phishing, spearphishing and how to enhance e-mail and web security.

John Ward – Cyberblog November 2020

This is a process that is worth examining, and one which provides some insight into how the private and public sector can work together and combine resources to effectively combat, or at the very least, raise awareness regarding cybersecurity threats. In this case IBM, a private company, used their own resources to identify a cybersecurity threat. This information was then shared with the United States Government, in this case CISA, who used their resources to publicize the findings of the IBM X-Force to a wider audience and supplement the findings with their own independent resources. For some, adding the legitimacy of a federal agency under the auspices of the Department of Homeland Security may also add a level of legitimacy to the IBM X-Force's findings, and at the very least will add an increased level of visibility and awareness. Close cooperation between the federal government, who are allocated significant resources, and private entities, whom are usually the operators of large portions of America's critical infrastructure, is an imperative aspect of an effective cybersecurity strategy.

The IBM X-Force's findings also highlight an important aspect of critical infrastructure cybersecurity, in this case focusing on the healthcare sector. Many products, in this case the proposed COVID-19 vaccine (and also in most medical devices), there are tertiary concerns beyond the primary means of programming and assembly of the device/medication/etc… in question. These items must be shipped and stored, and that supply chain presents additional targets to motivated malicious actors. Even if a device or medication is designed with cybersecurity as a primary consideration, each additional stop, whether physical or digital, exposes that item to increased danger. Strong cybersecurity at the initial point of programming/assembly/development does not guarantee that the item in question is secure. Passing through other hands (or computers) before ultimate delivery to the front-end user creates a significant amount of risk that can undo any of initial cybersecurity considerations.

