March 24th, 2020

Hacking Healthcare

TLP White

In this edition of Hacking Healthcare, we take an in-depth look at telework. As the spread of COVID-19 has led to social distancing and other policies meant to curb infection rates, many industries are turning to telework to continue operations to the maximum extent possible. Below we outline some of the general challenges of this transition, as well as some specific difficulties the healthcare sector faces in adopting both telework and telehealth. And speaking of which, we start with an announcement from the US National Institute of Standards and Technology (NIST) on their new telehealth initiative. Welcome back to *Hacking Healthcare*.

NIST NCCoE's "Securing Telehealth Remote Patient Monitoring Ecosystem" Project: The National Cybersecurity Center of Excellence (NCCoE) at NIST has moved the *Securing Telehealth Remote Patient Monitoring Ecosystem* project into the build phase after accepting letters of interest from the private sector. The project's stated goal is to "provide a reference architecture that will address the security and privacy risks for healthcare delivery organizations (HDOs) leveraging telehealth capabilities such as remote patient monitoring (RPM)."[1] The need for such guidance has increased in recent weeks as the benefits and use cases of telehealth have become apparent during the COVID-19 pandemic

Ultimately, NIST plans on publicly releasing a Cybersecurity Practice Guide that will provide "detailed implementation [guidance regarding] practical steps needed to implement a cybersecurity reference design that addresses" the challenges inherent in telehealth.[2] The organizations partnering with NIST on this project include Accuhealth, Cisco, Inova Health System, LogRhythm, MedCrypt, MedSec, Onclave, Tenable, University of Mississippi Medical Center, and Vivify Health. More information, including a full project description, can be found on the NIST NCCoE website.[3]

The Telework Transition: The speed at which COVID-19 went from concern to crisis caught many organizations off-guard. The sudden need to protect employees and communities by complying with health recommendations like social distancing has turned telework from luxury into necessity for many companies and government agencies needing to continue operations. While this transition has mitigated some of the economic impact that might normally be associated with such dramatic circumstances and allowed the continuation of many essential services, teleworking has its own unique challenges that need to be carefully managed.

Security

Among the most significant issues that all organizations will face as they attempt to embrace telework is how to remain secure. Securing on-premises networks is already a challenge for thinly resourced IT teams. The added complexity of quickly scaling up secure remote access organization-wide cannot be understated. Recognition of this fact even led NIST's Information Technology Laboratory (ITL) to release a bulletin outlining specific security concerns surrounding telework and remote access.[4]

In that bulletin, NIST acknowledges that telework and remote access technologies increase exposure to malicious threats and require additional protections. They specifically call out the following:[5]

1) *Physical Security*: Additional risk of compromise due to mobile devices being off premises in uncontrolled environments
2) *Unsecured Networks*: Increased risk is associated with the use of external networks
3) *External Access to Internal-only Resources*: Increased risk is associated with remote access to sensitive internal resources

NIST recommends that organizations build their remote access telework security policies and controls with the assumption that devices will be exposed to external threats. They also suggest that telework security policies should clearly define requirements for working remotely, remote access servers should be correctly configured and effectively secured to enforce security policies, and that organization-controlled telework devices should be secured against common threats. One of the most effective ways of enabling that security is through multi-factor authentication (MFA). The vast majority of VPNs and online application support MFA and this should be enabled wherever possible. The ITL bulletin goes on to list several NIST documents that give more comprehensive guidance on these issues.

Capacity

Capacity may also be a major hurdle to clear for many. Whereas telework in the past has generally been reserved for specific individuals, specialized tasks, or uncommon events, the sudden need to bring an entire organizational workforce or student body online has exponentially increased capacity needs across a wide spectrum of use cases. A shortage of secure take-home devices; limitations to servers and underlying infrastructure; a shortage of IT professionals to support a mass transition; and a lack of reliable low-cost, large-scale communication technologies are some of the factors cutting into the efficiency of telework.

Reports from both public and private organizations in many industries note that they simply can not scale-up to meet demand. For example, earlier this month, the U.S. Airforce's virtual private network (VPN) software was limited to 72,000 connections at a time, far short of the roughly 275,000 civilian workers and full-time contractors that they employ.[6] While, the U.S. Air Force might have the means to scale up relatively quickly, many organizations do not have the resources.

Zscaler's CISO, Stan Lowe, noted that even those organizations that do have significant remote capabilities typically have the VPN infrastructure to support only 20-30% of their workforce remotely.[7] He elaborated that scaling up can be costly and time consuming as hardware needs to be bought, shipped, deployed, and then updated and maintained.[8] In his estimation, it can take months to successfully implement everything required to smoothly transition an organization to a primarily telework model.[9]

Availability

A further complication of the unexpected shift to telework is availability. The FCC's *2019 Broadband Deployment Report* estimates that over 21 million Americans do not have access to broadband Internet connections.[10] Broadband Internet connections are defined by the FCC as having at least 25 Mbps download rate and 3Mbps upload rate, and low Mbps can significantly impact file transfer rates and audio/video communication. At a time when households are recommended or required to remain indoors, the bandwidth that is available to these households is often stretched thin by multiple individuals competing for usage.

Healthcare and Public Health

In the healthcare and public health sector, telework and telehealth are currently more valuable than ever for providing a means for healthcare professionals interact with patients who are sheltering in place or would be exposed to significant risk by physically visiting a healthcare facility. It can also mitigate the risk to healthcare providers who are not on the immediate frontlines of the COVID-19 response. Furthermore, it allows those healthcare providers who may be quarantined to still provide necessary aid.

However, while many of the technologies to enable high quality telehealth and telework exist, few healthcare organizations have invested substantially in acquiring and training personnel on those capabilities. While investment in medical tech like telehealth technologies has been slowly growing over the years, COVID-19 has shown how much more needs to be done.[11] To further integrate telehealth and telework into their systems, healthcare organizations will have to tackle a few challenges.

First, as a highly regulated industry with a premium placed on preserving the privacy and security of patient data, telework and telehealth must contend with numerous legal and regulatory demands, such as HIPAA and other legal regimes. While the Health and Human Services Department (HHS) has recently relaxed enforcement around some of these protections in an effort to combat COVID-19, healthcare organizations must remain vigilant that their practices are compliant with laws and attentive to new privacy concerns.[12]

Second, there is also an issue of resources. Under normal circumstances, it can be difficult for healthcare organizations to find the resources to invest in things like telework and telehealth that could be deemed a luxury. However, at a moment when teleworking and telehealth technologies are perhaps most beneficial, resource allocation for such efforts are in direct competition with the need to purchase medical equipment like ventilators and masks, re-tool for the fabrication of medical equipment, and contend with the reality of a sharp downturn in the economy. Strained resources in the present environment have taken a toll on HDOs in their efforts to efficiently and effectively roll out telework and telehealth capabilities.

For healthcare organizations that are in the midst of dealing with the issues outlined above, rest assured that various entities are working to disseminate documentation to assist during the transition. In addition to the comprehensive general guidance that NIST provides, the Healthcare and Public Health Sector Coordinating Council (HSCC) has also recently released guidance. Entitled "*Management Checklist for Teleworking Surge During the Covid-19 Response*," (https://healthsectorcouncil.org/covid-checklist/) the document is "designed as a quick reference for healthcare enterprise management to consider important factors in a teleworking strategy that minimizes downtime and latency while supporting patient care, operational and I.T. security, and supply chain resilience." It is freely available on the HSCC website, and we encourage you to read through it.

Conclusion

Telework and telehealth are unexpectedly experiencing the largest possible test to date with little notice for organizations to prepare themselves. While we are still only a few weeks into this situation, the early findings suggest that teleworking and telehealth are having a noticeable impact. There are limitations, but many of the initial challenges outlined above appear to be solvable with maturation of technology and telework policies. While the health effects of COVID-19 will resonate for years, it seems plausible that one of its longest legacies it will be a shift in how the world embraces these technologies.

Congress –

Tuesday, March 24th:
- No relevant hearings

Wednesday, March 25th:
- No relevant hearings

Thursday, March 26th:
- No relevant hearings

International Hearings/Meetings –

EU – No relevant hearings/meetings

Conferences, Webinars, and Summits –

--H-ISAC Monthly Member Threat Briefing – Webinar (3/31/2020)
https://h-isac.org/hisacevents/h-isac-monthly-member-threat-briefing-6/
--H-ISAC Security Workshop - Frederick, MD (6/9/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-frederick-md/
--AAMI Exchange – New Orleans, LA (6/12/2020-6/15/2020)
https://h-isac.org/hisacevents/aami-exchange/
--H-ISAC Security Workshop - Lisbon, Portugal (6/17/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-lisbon-portugal/

--H-ISAC Security Workshop - Buffalo, NY (6/23/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny-2/
--H-ISAC 2020 Inaugural APAC Summit – Singapore (6/23/2020-6/25/2020)
https://h-isac.org/summits/apac-summit-2020/
--Healthcare Cybersecurity Forum - Rocky Mountain – Denver, CO (7/20/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426499
--Healthcare Cybersecurity Forum – Southeast – Nashville, TN (9/9/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/426517
--H-ISAC Security Workshop - Greenwood Village, CO (9/16/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-greenwood-villiage-co/
--Healthcare Cybersecurity Forum – Northeast – Boston, MA (9/22/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/427126
--Summit on Security & Third Party Risk – National Harbor, MD (9/28/2020-9/30/2020)
https://h-isac.org/hisacevents/summit-on-security-third-party-risk/
--Healthcare Cybersecurity Forum – Texas – Houston, TX (10/8/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428840
--H-ISAC Security Workshop - Mounds View, MN (10/27/2020)
https://h-isac.org/hisacevents/h-isac-security-workshop-buffalo-ny/
--Healthcare Cybersecurity Forum - Pacific Northwest – Seattle, WA (10/28/2020)
https://endeavor.swoogo.com/2020_healthcare_innovation_cybersecurity_forums/428886
--Healthcare Cybersecurity Forum – California – Los Angeles, CA (11/12/2020)
https://h-isac.org/hisacevents/healthcare-cybersecurity-forum-california-2/

Sundries –

--Russian hackers using stolen corporate email accounts to mask their phishing attempts
https://www.cyberscoop.com/fancy-bear-phishing-email-trend-micro-apt-28/
--Ransomware claims more than doubled in the last year
https://www.cyberscoop.com/ransomware-beazley-insurance-claims/
--Windows code-execution zeroday is under active exploit, Microsoft warns
https://arstechnica.com/information-technology/2020/03/attackers-exploit-windows-zeroday-that-can-execute-malicious-code/
--UK coronavirus app 'must respect privacy rights'
https://www.bbc.com/news/technology-52003984

Contact us: follow @HealthISAC, and email at contact@h-isac.org

[1] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth
[2] https://www.nccoe.nist.gov/projects/use-cases/health-it/telehealth
[3] https://www.nccoe.nist.gov/sites/default/files/library/project-descriptions/hit-th-project-description-final.pdf
[4] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf
[5] https://csrc.nist.gov/CSRC/media/Publications/Shared/documents/itl-bulletin/itlbul2020-03.pdf
[6] https://www.cnn.com/2020/03/20/tech/telework-security/index.html
[7] https://www.scmagazine.com/home/security-news/news-archive/coronavirus/vpns-not-a-cybersecurity-slam-dunk-for-telecommuters-in-the-age-of-covid-19/
[8] https://www.scmagazine.com/home/security-news/news-archive/coronavirus/vpns-not-a-cybersecurity-slam-dunk-for-telecommuters-in-the-age-of-covid-19/

March 24th, 2020

[9] https://www.scmagazine.com/home/security-news/news-archive/coronavirus/vpns-not-a-cybersecurity-slam-dunk-for-telecommuters-in-the-age-of-covid-19/

[10] https://docs.fcc.gov/public/attachments/FCC-19-44A1.pdf

[11] https://pitchbook.com/news/articles/telehealth-could-be-at-the-heart-of-a-new-beat-in-vc-backed-healthtech

[12] https://www.hhs.gov/hipaa/for-professionals/special-topics/emergency-preparedness/notification-enforcement-discretion-telehealth/index.html