September 14th, 2021

TLP White

This week, *Hacking Healthcare* begins by diving into a new report that highlights the growing tension and dissatisfaction between security teams, employees, and leadership when addressing remote work and cybersecurity. We pull some useful insights from the report and pose some questions that may help alleviate similar issues within your own organization. Next, we wrap up with a breakdown of a cloud misconfiguration report and make a case for the utility of harnessing the independent security researcher community.

Welcome back to *Hacking Healthcare*.

1. **The Tension Between Security and Remote Work**

   The rapid exodus to remote work for a large percentage of individuals created numerous security headaches for many organizations with little time to address them. The sudden shift required adjustments to processes, policies, and capacity in order to ensure that security and privacy was maintained in the face of new and expanded types of cyber risk. A new study conducted by Hewlett-Packard (HP) suggests that this "new normal" has yet to find an agreeable balance between business considerations, workforce expectations, and security and privacy realities.

   Published on September 9th, HP's 13-page *Rebellion & Rejections Report* shines a light on what appears to be widespread tension among remote workers and organizations. With COVID-19 showing resiliency and roughly ~39% of office workers globally expecting to at least split their time between working remotely and being in the office even after COVID-19, it seems unlikely these issues can be ignored.[1] What exactly did the report find?

   Among the workforce:[2]

   - For younger office workers (18-24 years):
     - 39% "were unsure of the existing data security policies in place at their work"

  - 54% were more concerned "about deadlines than exposing the business to a data breach"
  - 48% think "security policies are a hindrance"
  - 31% had "tried to circumvent security

- More generally, 37% of office workers think security policies and technologies are too restrictive and 48% think they waste a lot of time

And among security and IT teams:[3]

- Security leadership is only growing in importance, and a positive security culture must be central to the organization

- 91% "felt pressure to compromise security for business continuity" – with 50% saying the pressure they felt was "significant"

- 83% believe "home working has become a 'ticking time bomb' for a network breach"

- "83% of IT teams said trying to set and enforce corporate policies around cybersecurity is impossible now that the lines between personal and professional lives are so blurred"

- 80% believe IT security has become a "thankless task"

All of these statistics combine to paint a dreary picture. As the report summarizes, workforce aggravation and IT/security disaffection are a troublesome mix for a complex security environment in which threats are evolving and scaling up.

While it appears likely that workforces will continue to slowly increase their in-person presence in the coming months, it's difficult to imagine that remote work isn't here to stay to a significant degree. And as we have discussed previously, this move to more remote work didn't just arrive with the pandemic. Many industries were already trending in that direction as the technology to make work-from-home successful came along. With that in mind, some new approaches are needed to ensure organizational security, business priorities, and workforce expectations can coexist.

Action & Analysis
Membership required

2. Cloud Misconfiguration Report Highlights Role of Security Researchers

The continued adoption of cloud computing within all sectors speaks to the power and benefit that can be derived from the technology, but it brings with it a unique set of security and privacy challenges. As the usage of cloud technologies and services

increases, the risk of improper configurations resulting in sensitive data exposures climbs along with it. The results of a recent report from cybersecurity company Rapid7 contained some interesting insights into this issue that are worth noting for the healthcare sector.

Rapid7's *2021 Cloud Misconfigurations Report* set out to "look at 121 publicly reported data exposure incidents that were disclosed in 2020" with the goal of finding "common causes and circumstances among them."[4]

The report's findings included:[5]

- Healthcare was one of the most represented of the 15 industry sectors within the sample, and the combined records exposed touched on 13 of the 14 record types used by the study (*e.g.*, Financial, Credentials, Location, Photo/Media)
- 62% of the incidents in the study were discovered by independent researchers
- ~45% of the reported exposures were due to insufficiently protected Amazon Simple Storage Service (S3) buckets (~25%) and Elasticsearch databases (~21%)
- In 2020, there were on average 10 disclosed incidents of this type per month

In the report's conclusion, Rapid7 called attention to the fact that it is common for individuals to actively seek out cloud service misconfigurations and that it isn't terribly difficult to find them. They recommend that organizations in all sectors take care to assess what data they are exposing to cloud services and to note which configurations are secure, resilient, and appropriate for a given use case. Additionally, they recommend that organizations ensure that automated processes are in place to monitor the configurations.

Action & Analysis
Membership required

Congress –

<u>Tuesday, September 14th</u>:
- House of Representatives - Committee on Science, Space, and Technology: The Disinformation Black Box: Researching Social Media Data

<u>Wednesday, September 15th</u>:
- No relevant hearings

September 14th, 2021

Thursday, September 16th:
- No relevant hearings

International Hearings/Meetings –
- No relevant meetings

EU –

Conferences, Webinars, and Summits –

https://h-isac.org/events/

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

---

[1] https://threatresearch.ext.hp.com/wp-content/uploads/2021/09/HP_Wolf_Security_Rebellions_and_Rejections_Report.pdf
[2] https://threatresearch.ext.hp.com/wp-content/uploads/2021/09/HP_Wolf_Security_Rebellions_and_Rejections_Report.pdf
[3] https://threatresearch.ext.hp.com/wp-content/uploads/2021/09/HP_Wolf_Security_Rebellions_and_Rejections_Report.pdf
[4] https://www.rapid7.com/c/cloud-misconfigurations-2021/
[5] https://www.rapid7.com/c/cloud-misconfigurations-2021/