Proprietary Software and Security

By Roy Schestowitz
Created 26/08/2021 - 10:45am
Submitted by Roy Schestowitz on Thursday 26th of August 2021 10:45:49 AM

- [Microsoft’s Power Apps leaks data from 47 companies, report finds](http://www.tuxmachines.org/content/proprietary-software-and-security#3)

  In June, UpGuard researchers submitted a vulnerability report to Microsoft Security Resource Center (MSRC), addressing the issue of OData feeds identification as it provides unidentified admission to a selection of data and URLs for accounts that were potentially exposing critical data.

- [Cyberattack Forces Memorial Health System to Divert Patients to Alternate Hospitals](http://www.tuxmachines.org/content/proprietary-software-and-security#4)

  Memorial Health System operates three hospitals in Ohio and West Virginia, all of which have been affected by the attack. Since electronic health records were not accessible, patient safety was potentially put at risk, so the decision was taken to divert emergency patents.

- [Memorial Health System recovers from ransomware](http://www.tuxmachines.org/content/proprietary-software-and-security#5)

  In a bulletin posted on its site, healthcare facility network Memorial Health System, based in West Virginia and Ohio, said it was beginning the process of recovery and restoration after being hit with a ransomware attack earlier in the week. The network reported on Sunday that it experienced an “information technology security incident” that caused it to suspend all online access across its 64 clinics, including hospitals Marietta Memorial, Selby General, and
Sistersville General. Surgeries have been canceled, ambulances have been diverted, and clinic staff have had to work with paper charts. But on Wednesday, the network announced it had reached a "negotiated solution," and that it is "beginning the process that will restore operations as quickly and as safely as possible."

**By Design: How Default Permissions on Microsoft Power Apps Exposed Millions**[6]

We had discovered over a thousand anonymously accessible lists across a few hundred portals that needed to be analyzed and potentially notified. Ideally, Microsoft would have been involved in doing so, but our attempt to pursue this option thus far had been unsuccessful—though Microsoft would later take action after we had notified some of the most severe exposures. We spent the next few weeks analyzing the data for indicators of sensitivity and reaching out to affected organizations. The notification timelines and data classes for some of the most significant exposures are described below to give a sense of the prevalence and impact of this design decision.

**Cybersecurity company flags Microsoft Power Apps data leak of 38M records**[7]

The types of data included names, email addresses, personal information used for COVID-19 contact tracing, COVID-19 vaccination appointments, Social Security numbers for job applicants and employee IDs.

**Cyber insurance market encounters "crisis moment" as ransomware costs pile up**[8] [iophk: Windows TCO]

Two separate CEOs of major insurance giants remarked in recent weeks about a considerable jump in cyber insurance premium prices: AIG's chief executive said rates increased by 40% for its clients, while Chubb's chief executive said that company was charging more, too.

Rather than welcoming the trend, Chubb CEO Evan Greenberg offered a warning. Those price increases, he said, still don't reflect the grave risk that a catastrophic cyber event poses. "That is not addressing by itself the fundamental issue," he said.

**Healthcare provider expected to lose $106.8 million following ransomware attack**[9] [iophk: Windows TCO]

The bulk of the losses, representing $91.6 million, came from lost revenues during the four weeks the organization needed to recover from the May ransomware attack.
Scripps also lost $21.1 million in costs associated with response and recovery. While the company said it recovered $5.9 million through its insurance policy, the healthcare provider said it expects to lose an estimated $106.8 million by the end of the year.

The losses stemming from the ransomware attack do not include potential losses due to litigation.

- The pandemic revealed the health risks of hospital ransomware attacks

The findings, which are still unpublished, should help push back on any groups hesitant to say that cyberattacks are dangerous for patients, says Josh Corman, a senior adviser to CISA, the federal agency that advises on government and private sector cybersecurity issues. “We should stop pretending that there is no harm to human life from cyber attacks,?” he says.

- Microsoft Is Going to Make it Difficult for Chromebook Owners to Use Word Offline

About Chromebooks reminded me there is an Office Editing extension from Google that lets you download Word, Excel, and PowerPoint files to edit with Google Docs, Sheets, and Slides. It enables you to edit those files in Google Docs without the [Internet], and it stays dormant in the background until it senses an active connection, when it then uploads your changes. There are also open-source alternatives to opening and editing Office files, namely the Linux version of LibreOffice, a relatively easy install on the Chromebook if you’re not intimidated by Linux apps.

Source URL: http://www.tuxmachines.org/node/154925

Links: