Julian Garcia

CSE 489

August 31, 2021

Two articles on Cybersecurity

1. ***'Surveillance state': Australian police given sweeping new hacking powers***

   Article Link:

   https://cointelegraph.com/news/surveillance-state-australian-police-given-sweeping-new-hacking-powers

   This article details new legislation enacted in Australia which gives authorities the power to run hacks on any individual or group, provided they have a warrant to do so.
   "The new warrants authorize police to hack the personal computers and networks of suspected criminals, seize control of their online accounts and identities, and disrupt their data." There's some concern with this kind've legislature, in that the limits of who they can really seize data from and why are defined vaguely. In proposing the legislature it was advised that issuing these warrants for hacking be limited to events where there criminals have commited "offenses against national security, including money laundering, serious narcotics, cybercrime, weapons and criminal association offenses, and crimes against humanity", but the actual legislation left out this prerequisite, and so there's concern about what data may be seized, who may be hacked, and how ethically these events will be.

2. ***This Agency's Computers Hold Secrets. Hackers Got In With One Password.***

   Article Link:

   https://www.nytimes.com/2021/06/18/nyregion/nyc-law-department-hack.html

This article details how New York City's Law Department network was penetrated through a single worker's login information, which hackers acquired. This attack could've been prevented completely through implementing multi-factor authentication, which is one simple safeguard that most other services (even those with much less valuable data) implement. The Law Department failed to implement multi-factor authentication despite it being "more than two years after the city began requiring it", and the consequences of this failure "interrupted city lawyers, disrupted court proceedings and thrust some of the department's legal affairs into disarray." The authorities still have no idea what the motive of the attack was, or even how extensive it was, all they've done so far is disconnect the department's computers from the city's wider network.

Exam Questions:

1. Relating to what we talked about in class, what could be done to ensure that New York City's wider network is safe to use?

   Answer: Considering they don't have a complete idea of the scale of the attack, the only way to be sure would be to purge all systems completely and start anew.
2. (Open ended) Should there be limits on state-sponsored hacking for the sake of investigating crime? Explain your reasoning.