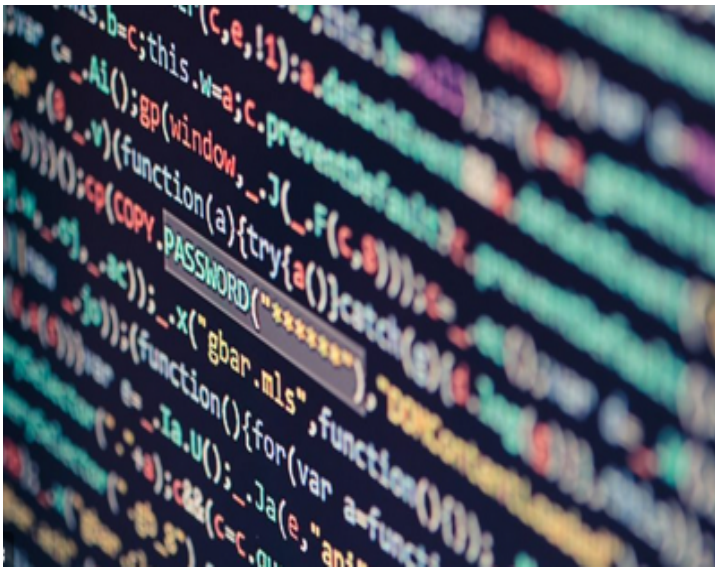
BLOCKNUBIE

Security of Electronic Health Records



Lately, we all have read in the news about security incidents. Sometimes hackers (organizations or individuals),) steal data as it happened to Anthem Inc that ended up paying 39.5M USD, others encrypt the data and ask for ransom (University Hospital New Jersey) and others they just take money from organizations (as in the Swiss University)or individual accounts. The Healthcare industry, if by far one of the most affected by the hackers' attacks, they have reported over the last months over three successful attacks per day. The stakes are higher: healthcare institutions have a lot of personal data, far more than financial institutions. Hackers can steal that valuable data, but they can also encrypt it and make it inaccessible, and that put life's at risk. Is not only about the economic and legal, it is also a significant health risk. That push the HC providers to pay ransoms more than others industries. In late September they have shutdown computers at Universal Health Services in the US and also at Düsseldorf University Hospital in Germany.

The cost of Data breaches has been increasing year to year around 6.5%. The healthcare industry is one of the most susceptible to the hackers' activity. This susceptibility is evidenced in the cost of data breaches: the HC industry has the highest average cost per attack: 6.5M €. Even the cost of each record stolen is three times the cross-industry average, around €408 per stolen record.
Hackers are, at the end of the day, criminals who want to maximize their profits, and they know that patient data is extremely valuable. They are looking for detailed identity information, and that data is present in electronic health records (EHRs). Hackers can not only steal but also make unavailable (ransomware) the EHR's and that also has a potential impact on the patient's wellbeing. At last but not least, the HC industry sensibility makes it also a target for hostile states attacks, as in the case of the HC sector in Australia who has been under attack by sophisticated attacks for months. Just those three threats should be enough to bring awareness to the HC industry and start taking serious steps to secure the health record, and personal details should be a top priority in the healthcare industry.

Why Hackers care so much?

There is a question that begs to be asked: Why common hackers will care so much about EHR's? As it was said once, "It's economics, dummy". A quick search in the dark web shows that EHR are, by far, the most expensive records that you are sold online. Today you can buy credit card data starting in €12, hacked social media accounts for less than a hundred € and hacked PayPal account for €300. Complete EHR can reach over a thousand € making it one of the most valuable assets to stole for hackers. The second factor is unfortunate but true, banks and financial institutions have spent lots of time and resources (technology and specialist) in stepping up their security, most healthcare institutions have not. The combination of relaxed security standards, unawareness, high prices in the black market and the digitalization trend is the perfect opportunity to be exploited by unscrupulous hackers.
The pandemic has exacerbated the situation: Elite hackers have attacked governments and international organizations working on pandemic response. The World Health Organization was targeted in March by "unknown" attackers who attacked the organization with phishing messages in an attempt to access its digital systems. Also, hackers believed to be linked to Iran have targeted staff drugmaker Gilead, as the company works a treatment for the COVID-19 virus. Cybercriminals are creating thousands of new sites every day to carry out spam campaigns, phishing, or to spread malware. Cybercriminals are taking advantage of the increase in global communications due to coronavirus to mask their activities. Malware, spyware and Trojans have been found embedded in interactive coronavirus maps and websites. Spam emails are also tricking users into clicking on links which download malware to their computers or mobile devices. Besides the increased attacks, there are fewer resources and increased risks. IT and security team have not only been depleted by the pandemic (as in any other profession) but also have been expending lots of effort to keep most of the employees working remote. Keeping a lot of people working remote takes a toll on the IT teams and working remote without proper preparation increases the security risk. Less personal available, more work, increased security risk and increased access to records added to create the perfect storm for the security of EHR's.

Another valid question to ask why someone will pay that much for HER's? A complete health record includes a full name, address, contact information, social security number (or equivalent), insurance details, the name of treating physicians, diagnoses, prescriptions, and much more. That in itself is less than a curiosity, but using all that data the buyers can commit many frauds: can usurp the identity to open bank accounts, get credits cards and loans and get restricted prescriptions that can be sold for hundreds of euros each. At last but not least, EHR cannot be voided or canceled as credit cards and bank accounts. The loss is permanent and the data can be re used again and again.