Henry Post

ITMS 428

# What is Cybersecurity, and what is Database Security?

Cybersecurity could be described as a collection of skills, concepts, and knowledge about computers. It is a very popular term, and like many others, can be nebulous and loosely-defined. Definitions across different governments and nation-states are inconsistent, conflicting, redundant, or simply use different words to describe similar things. Unfortunately, this problem also exists across multiple industries and throughout the academic world. (**Schatz, Daniel**)

Despite all the differences in the precise definition of ‘cybersecurity’, there are common themes in everyone’s definition. The idea of being connected to the internet, having a large number of separate ‘devices’ connected to a service or website, defending against threats that exploit flaws in your application or something your application trusts, etc. are all things one finds discussed when talking about cybersecurity. If I were forced to use one short sentence to describe it, it would be as follows:

“Cybersecurity is about controlling unauthorized access to digital systems.”

Cybersecurity does indeed cover many fields within the context of computers and digital information. It has to do with the flow of information, websites, databases, credentials, to name a few concepts. It spans across all of the physical and virtual components of a system, hence why so many things are involved. For example, your company could have quite an impressive firewall and intrusion detection system, as well as armed guards and cameras everywhere. However, all it takes is a curious employee picking up a flash drive from the parking lot to possibly nullify all of that work.

Cybersecurity as it pertains to database systems is a narrower topic, and (hence the term) is focused on databases. These are, simply put, systems which store large amounts of data. They can be as innocuous as your favorite songs on Spotify, perhaps what you rated movies on imdb, or something more sensitive like your credit card number (as is stored on any site which saves it).

The priorities when talking about database security are a little more narrow, too. You want to ensure that your database system is secure when accepting data from users, one common exploit being ‘SQL Injection’. There is also the possibility of being given data that can cause you to send raw memory out, a famous example of this being the “Heartbleed” bug that affected the OpenSSL library that let users read very small amounts of memory from a target. There is also a similar exploit called “buffer overflow” that allows attackers to *write* to memory instead of *reading* from it.

The exploits described are not immediately intuitively understood. At times, it’s near impossible to anticipate where a vulnerability may lie. However, being well-versed in the software and technologies that go into making a database will help one anticipate these threats. Certain common themes might emerge, such as handling user input, transporting data safely, how you store data, and staying up-to-date on discovered exploits. These topics all show up repeatedly when popular data breaches (such as EquiFax) happen.

Indeed, EquiFax did not have just one flaw. It reports, officially, that a (patched) flaw in ‘Apache Struts’, an open-source application, was exploited (**NVD - CVE-2018-11776**) to execute code remotely. This is an example of failing to update vulnerable software. However, another issue (insecure storage of credentials) was revealed. **Mann, Bill** describes how researchers were able to view the public source of an Argentinian Equifax branch’s website page, and to their surprise, see the passwords and usernames of about 100 employees.

It’s not all about *preventing* access to systems, as there is some inevitability to this. Perhaps your database is affected by a previously undisclosed (zero-day) exploit. What can one do if your system is compromised? Well, certain actions can *mitigate how much useful information* an attacker can get from a successful breach.

Suppose you are EquiFax, and you actually encrypt all of your customer’s data using their password. You don’t store their password, nor do you store their password’s hash. A successful login attempt is verified when their information is decrypted, and none of the decrypted info is ever written to disk.

Let’s say the breach occurs, only this time, the attackers may get perhaps 10,000 decrypted credentials from a memory dump, and millions of entries of entirely useless, encrypted credit data that would take centuries to decrypt.

You can still mitigate damage even if you don’t encrypt anything, by setting up your applications and services in a way that restricts the scope of each application with respects to all others. Suppose your user information system has its own database and cannot access the password database, nor the payment information database. This way, if an attacker gains access to the user info database, they cannot get password hashes or payment information.

What can we take away from this? One conclusion is that cybersecurity, even just in the context of databases, can be concerned with a wide variety of systems and topics. Its concerns can include websites, how users authenticate themselves, how and where their data is stored, any and all libraries your business uses, and how much priviledges you give to entities you trust (such as the security standards of the people who host your website).

However, database security’s concerns aren’t hopelessly broad. By understanding the technologies that cybersecurity and database security use, one can begin to narrow down the area of potential threats one wishes to focus on. Common, well-documented and known-problem areas are a good starting point if one wants to know what concerns database security should cover.

Citations

Schatz, Daniel, et al. “Towards a More Representative Definition of Cyber Security.” *Scholarly Commons*, <https://commons.erau.edu/jdfsl/vol12/iss2/8/>.

“What Is Cybersecurity?” *Cisco*, 24 Aug. 2018, [www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html](http://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html).

“Introduction to Cyber Security.” *UMUC*, [www.umuc.edu/academic-programs/cyber-security/about.cfm](http://www.umuc.edu/academic-programs/cyber-security/about.cfm).

“CVE - CVE-2014-0160.” *CVE - Search Results*, <https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2014-0160>.

Mann, Bill. “A Lesson in Secure Password Management from the Equifax Data Breach.” *Secure Thinking by Centrify*, 21 Aug. 2018, <https://blog.centrify.com/secure-password-management-equifax-breach/>.

“NVD - CVE-2018-11776.” *NVD - 800-53*, <https://nvd.nist.gov/vuln/detail/CVE-2018-11776>.