4 key takeaways from the 2022 Verizon DBIR report - Infosec Resources

Keatron Evans

8-10 minutes

Last month was a holiday of sorts for the cybersecurity community – the release of Verizon's annual Data Breach Investigations Report. This year's 108-page report analyzed over 23,000 incidents and 5,200 confirmed breaches from around the world.

As many cyber pros do, I sat down to read the full report (over many cups of coffee). As an ethical hacker and cybersecurity instructor with over 17 years in the business, here are some of my top takeaways from the report.

1. Supply chain is still top of mind and a serious threat

When we look at the other top items on the list from this report, they are intrinsically linked to the supply chain. Several high-profile ransomware attacks were at the hands of vendors or suppliers. Several intrusions not involving ransomware were due to vendors and suppliers.

It's great to see this report finally confirm this, but we're still not any closer to a solution than we were when the "Winds of Solar" supply chain breach shook the world.

2. 82% of actual breaches had a human element to them

Social engineering, primarily phishing, still leads the way for most data breaches. Credentials fall right behind it. But it's worth mentioning the relationship between the two. Often times the reward of successful phishing is credential harvesting. This keeps end-user security awareness, endpoint protection and EDR solutions in the lead as the best weapons to defend against the leading breach avenues.

There is also a mention of pretexting and business email compromise being key drivers for this. I can cite our own internal numbers. Out of all of my clients, and companies with 100 or more employees, we've had to assist with business email compromise attacks against at least one executive at each organization. So this mirrors what we are seeing at our own micro-level.

3. Threat actors' dwell time may not actually be improving

One of the things we like to cite in the world in incident response and threat hunting is dwell time, or delta-time as it is sometimes referred to. It is essentially the amount of time between when your environment is first breached and when you first find out about it.

The average has hovered around 85 to 100 days for a while now. I remember reading the Verizon DBIR report back some years ago and being shocked at not only the amount of times that passes, but the fact that at that time, law enforcement notification was the lead method for victims finding out they were breached. It will be equally shocking for some to know that threat actor notification is one of the top methods these days. Yes, you read that right, the organization knows because the hackers notified them. This is mostly due to ransomware.

The biggest and scariest question here is this: How long would these organizations have been compromised before they found out had not the attackers notified them. A side effect of this expedited attacker notification of a breach is it makes it appear we are trending in the right direction as far as dwell time, as one might get excited about the fact that the time from breach to notification is down. But we have to put it into context.

On the surface, this seems like a good thing, but if we connect this to the point that a big percentage of data breaches reported were ransomware, the victims found out quickly because the attackers literally told them, by demanding ransom. So it may be that the improvement in dwell time or delta-time is directly a result of ransomware operators wanting to get you notified quickly, so they are able to get paid quickly.

4. System intrusion is still effective, penetration testing is still needed

The process of how services and vulnerabilities are discovered and exploited has not changed at all.

Back in 2003 when I took my very first ethical hacking course, one of the things drilled into my mind by Jack Koziol was discovery scan, port scan, service identification and research the exploit. To this day it is the foundation on which most ethical hacking is taught. And per the report, this is still what is being viewed as the primary process system intrusion and exploitation.

In this regard, web applications are still a top vector for incidents, but an important metric here is when we compare incidents to actual breaches. This report considers incidents to be a “security event that compromises the integrity, confidentiality or availability of an information asset.” Whereas a breach is described as “an incident that results in the confirmed disclosure — not just potential exposure — of data to an unauthorized party.”

One of the most interesting points about this data is that when it comes to incidents. Web applications lead the way and are continuing to increase as the most observed attacks. However, when we break it down and apply the filter of just incidents that classify as data breaches, web application attacks are on the decline or going down. So the number of web application attacks is increasing when we look at incidents as a whole, but when those incidents are classified as breaches, which means when considering if the attack was successful, the number of web applications associated goes down significantly.

It could be that with the rapid migration to cloud services and the automation and modernization of front-end development, some of the low-hanging fruit web app vulnerabilities have disappeared. It could also be that web app development has gone all-in on security or any number of other things. I think it will take some time to figure out what this means. But it is interesting and worth consideration.

There are some positives though. For example, vulnerability remediation speed is up. This is undoubtedly a good thing.

Some final thoughts

Lastly, let me highlight the things that concern me the most. The number of system intrusions as related to incidents has remained flat. But the number of system intrusions related to breaches rose sharply. This could likely mean that the attackers are just getting better, and getting better quickly. It could also mean we're getting worse at defending those systems as there are some learning curves as we migrate these systems to cloud services, specifically, infrastructure as a service (IaaS) and platform as a service (PaaS) delivery models.

Another concern is that while we are improving on remediation, we are still remediating the same things. The vulnerabilities being exploited are not often zero-day in nature — they're well known and mostly patchable. A lot of the web application attacks, which seem to remain high, are based on stolen credentials. This blurs the actual issue: credentials are being stolen instead of bypassed by some advanced zero-day or next-generation attack.

It's no surprise that cybersecurity training has its own section in the report. There is a very timely mention of how long training can take depending on the outcomes. I tell students all the time. Getting certifications can happen quickly, but learning how to do something and execute it could take considerably longer. The statements made in this report about training developers and engineers on security since they build the systems are timely statements, and I believe they are right on point. This again echos my own data from our customers for whom we both train and provide penetration testing and other services.

I think there are many great pieces of data uncovered by this report. We have to stay diligent in removing low-hanging fruit vulnerabilities because even advanced threat actors are using them. We must make sure we keep our people trained up to be able to combat the latest threats.

I encourage everyone to read it on their own, while still thanking you for taking the time to read my opinions.

Reprinted from: https://resources.infosecinstitute.com/topic/4-key-takeaways-from-the-2022-verizon-dbir-report/