McBreach and The Automation Dependency: Undercooked Security Fundamentals in the Race for Bloated Efficiency and Convenience

Photo by Shahbaz Ali on Unsplash

Breach Overview

It was recently discovered that a breach of supersized proportion, impacting 64 million people was revealed. Two security researchers, Ian Carroll and Sam Curry, exposed vulnerabilities within the McHire recruitment site after reading Reddit posts from users complaining about the AI chatbot, Olivia, which was developed by Paradox.ai. After basic testing, which involved guessing weak usernames and passwords, the pair exposed an inactive account with active data using “123456” as login credentials. Further research led them to the third-party company Paradox.ai, which McDonald’s uses to automate the recruitment process on their McHire website. Applicant names, email addresses and phone numbers were accessed, leaving security professionals wondering how basic security fundamentals were overlooked. From weak password policies, governance and compliance ignored and an overall absent security posture, this breach is not only questioning the race to artificial intelligence, but highlights the lack of value and investment that companies place on cybersecurity.

Basic Security Fundamentals

In this case, basic security fundamentals were not implemented and at this time, there hasn’t been an explanation on why, only that new security measures will be implemented.

Through testing, the pair discovered weak usernames and passwords, indicating weak password policies. They also were able to access data without having to complete a multi-factor authentication process. Two basic, but critical security controls were not implemented while personal identifiable information (PII) of 64 million applicants were accessed. Based on the articles, there didn’t seem to be any additional security techniques implemented such as obfuscation.

- **Obfuscation** - Obfuscation is a security technique implemented to hide important data. It protects sensitive information making it harder for attackers to analyze or reverse-engineer.

Another key factor mentioned in this breach was that the account the research pair accessed had been inactive since 2019, however it had active data. This leads to several questions, however two glaring questions stand out.

- Why wasn't the account decommissioned much earlier?

Decommissioning is when IT assets are retired from active use and properly secured and disposed of.

- Why weren't there any security monitoring protocols in place?

If an account had been inactive since 2019, and not decommissioned, why weren't there any alerts or additional security parameters set to notify members of the security team that the "inactive" account suspiciously has activity after roughly five years.

With AI sparking a lot of buzz, the race for capitalism, and rapid development, security should not only be deemed as a first response to any event, it should be implemented in the development process. This incident is a blatant reminder that using guardrails, setting parameters, and testing are key. Responsible AI is only as responsible as those controlling the LLM, which could leave many to wonder if these new advancements can really be trusted.

From Inherent Trust to Zero Trust: The Gap is a Narrowly Large Paradox

On the subject of buzzwords, zero-trust rears its head in the context of this breach.

- Zero-Trust - a security framework that operates on the principle of "never trust, always verify."

Security professionals have been discussing what does zero trust actually mean, the implications on cyber environments, productivity, and how that looks from one organization to another, as it is not a one size fits all framework. However, it is established that implementing least privilege, segmentation, and no implicit trust are security factors that should be considered among others.

One thing all companies should consider, not just McDonald's is consumer inherent trust. When an organization trusts a third-party vendor with their data, applicants assume trust, but only based on the company they are dealing with, not necessarily the third-party.

In terms of McDonald's, users, more than likely, are not reviewing the terms of service and are not aware of service level agreements established with companies they've never heard of. They also, are probably not reading fine print statements, and inherently trust that McDonald's is handling their data properly. No organization should wholly trust third-party organizations and conducting due diligence is not only required, companies should want to ensure that the organizations they work with are in compliance. It might be an extra step, could even be considered cost and time consuming, however it does not compare to the costs and time that will be utilized to act against a breach by an attacker. In this case, lack of trust builds better business, and trust

The Blame Game is Easy...How to Re-Establish Trust

Publicity statements are great, but implementing security controls, strengthening security posture and implementing strong management and leadership mean more. Gaining trust from potential applicants, many of which probably consume the product is important, especially with distrust with AI. Maintaining trust, however, is much harder because it only takes one minor failure to lose it. While McDonald's has released a statement that shifts accountability to the third-party, they are not off the hook. Proper auditing and reporting should be a high priority when seeking third-party vendors to manage data. McDonald's

security teams should have conducted their own security tests to validate the vendors security compliance and abilities, and not solely focus on their ability to streamline and manage applicant tracking.

Paradox.ai released a statement in regard to a number of changes such as a bug bounty program, and strong password policies, but this is a little too late. Whether the account accessed was a test account or not, basic security controls should have been implemented, especially with active data on an inactive account.

With the chatbot being conversational, this is an easy opportunity for attackers to develop a phishing attack, leaving desperate applicants exploited. With these vulnerabilities caught by security researchers and not threat actors on the prowl, seizing an easy opportunity to gain additional PII such as social security numbers, banking information for future direct deposits, signature captures, and other information, companies should take heed of this breach and strengthen controls, if necessary.

The Race to Pseudo-Innovation

It's no secret that companies, students, and general users have flocked to AI for efficiency, convenience and even cheating. However various organizations have used services from big tech AI & Cloud providers to streamline their processes, cut costs, and increase bottom lines, while not considering security.

Capitalism and the race to be first, has made it possible to generate pseudo-innovation, while big business puts technical innovation under a heating lamp and shove it out the window as quickly as possible. This is how you end up with security breaches and potentially spending millions in damages. The race to innovation without proper testing and auditing leads to failure, and in this case, 64 million independent failures.

Conclusion

In the age of AI, the sprint to "innovation" and rapid technological advances, organizations cannot afford to be lazy in the way they implement cybersecurity controls. This is not just an opportunity for change for Paradox.ai, but also a chance for McDonald's to conduct proper auditing and reassess their shared responsibility model within their service agreements for the sake of conducting proper business across the board.

Overall, this breach presents the opportunity for organizations to not only place value on users and their data, but prioritize security before an attack happens.

Resources

- Bradley, T. (2025, July 17). *McDonald's AI breach reveals the Dark Side of automated recruitment*. Forbes. https://www.forbes.com/sites/tonybradley/2025/07/15/mcdonalds-ai-breach-reveals-the-dark-side-of-automated-recruitment/

- Wheeler, K. (2025, July 11). *How McDonald's AI bot exposed millions of peoples' data.* Cyber Magazine. https://cybermagazine.com/news/how-mcdonalds-ai-bot-exposed-millions-of-peoples-data