PASSWORD SECURITY – TIME FOR A NEW APPROACH?

Cyber-attacks on the health and research sector are becoming more sophisticated as the Australian Government calls for stronger protective measures.

Cyber-attacks in the healthcare sector are consistently listed at the very top of the industry sectors in the Australian Notifiable Data Breaches reporting, with recent figures revealing the sector registered nearly as many criminal breaches as the Finance and Legal/Accounting industries combined.[1]

The sector has recently seen an active surge in Advanced Persistent Threat (APT) Actors with the Australian Cyber Security Centre (ACSC) issuing an "advisory" in May this year. According to the Advisory (2020-009)[2], APT actors (organised entities and nation states):

"…pose the most significant threat to Australia's national security and economic prosperity"

and have,

"…been seen undertaking brute force attacks using a trial-and-error method to guess login credentials, and password spray attacks that attempt to access numerous accounts with a list of commonly-used passwords".

The numbers are escalating with recent allegations a state-based actor has been launching attacks on organisations involved in COVID-19 vaccine research with the aim of stealing information and intellectual property.

Password complacency is the common key to virtually all attacks with over 80% of hacking breaches being facilitated by weak, stolen, or predictable passwords.[3]

PASSWORD EDUCATION IS NOT SOLVING THE PROBLEM OF WEAK PASSWORDS.

According to the Verizon DBIR 2020 Report[4], using compromised credentials is still the easiest, and lowest cost avenue for attacks. While over 90% of Australians are aware that re-using passwords across multiple accounts is a major security risk, over two-thirds of us still recycle our passwords.[5]

The reality is that somewhere between 50% and 80% of passwords can be cracked easily and routinely, using tools available freely across the web. This is mainly due to weak and predictable passwords. Even more disturbing is that privileged accounts (those accounts providing access to high risk systems and information) are just as poorly maintained, meaning less effort is required by the attackers in gaining access to your core IP.[6]

PEN-TESTING IS NOT SOLVING THE PROBLEM OF WEAK PASSWORDS

Penetration-testing (Pen-testing) is a common practice to identify weak passwords. Pen-testing for weak passwords has more recently become a "tick the box" compliance process as the introduction of Privacy Laws (such as GDPR) has nullified the ability to enforce changes at the user-level.

Passwords are now "private information" so any pen-testing solution that reveals user passwords breaches privacy compliance.[7] Additionally, twelve percent of breaches are listed as insider attacks[8], increasing risk to users – especially since those users are likely to be re-using passwords in their personal security outside the organisation.

Since the purpose of passwords is to prevent unauthorised access to sensitive data and resources, the presence of weak passwords represents a GDPR compliance risk that, in itself, can result in significant fines.[9]

Unable to enforce and review, organisations can only request stronger passwords from their users, but with no visibility of changes, user behaviour is proven to revert to another weak password variation.

ALTERNATIVE AUTHENTICATION SOLUTIONS ARE NOT SOLVING THE PROBLEM OF WEAK PASSWORDS

While alternative authentication solutions, including Multi-Factor Authentication (MFA) and biometrics for example, add a layer of protection to weak passwords, they are, to some extent, plastering over the real issue - the weak passwords themselves. Additionally, these solutions are often incompatible with legacy systems, can take months to deploy, and become expensive to support.[10]

While alternative authentication solutions help in any defensive posture, they often provide a level of false confidence. Once penetrated, sophisticated attackers can easily work around these protections and weak passwords are quickly recovered and leveraged to gain deeper access.

PASSWORD POLICIES ARE NOT SOLVING THE PROBLEM OF WEAK PASSWORDS

The reason MFA and tokens have proven popular is that organisations have resigned themselves to the fact that they are unable to strengthen the passwords themselves…because, until now, true password resilience has been unachievable.

As a result, many industry experts are moving away from their "passwordless" narrative as the realisation sets in that passwords are here to stay, at least for some time to come. Industry experts including Gartner[11] are now advocating:

"… risk management leaders responsible for IAM should invest in other compensating controls in line with business needs"

PASSWORD HYGIENE VS PASSWORD HEALTH

Realising the need to strengthen passwords, admin teams introduced password policies designed to harden passwords against attack. While the intent is right, this solution does not generally inhibit attackers, while again providing a false sense of security to the business. Table 1 demonstrates the difference in password strength scoring based on policy versus actual password resilience against a simulated attack:

	THEORY	REALITY
Password	Password-Meter Password strength	Simulated Attack Password-Strength
Password123!	93/100	0/100
myC0m9anee1	86/100	12/100
P@$$word123!	100/100	18/100
Cuffcpf1811!	100/100	91/100
ToPS3cret	67/100	7/100

Table 1: Password Hygiene vs Simulated Attack Strength

This demonstrates a simple fact - attackers know about policies and simply apply "derivations" of simple passwords in their attacks. While "Password123!" meets most password policy guidelines, it is clearly a weak password against an actual attack.

This also highlights the risk of using derivatives of the same password across multiple accounts and simply adjusting that same base password whenever asked to change (e.g. "myp@ssw0rd11" is changed to "myp@ssw0rd22").

With the proliferation of compromised (leaked) credentials across the dark web, attackers now have access to a multitude of credentials pulled from previous data breaches. These passwords may be strong and compliant with the strictest policies, but if users tend to use the same passwords across their work and personal accounts, attackers can easily leverage this to compromise their work accounts.

THE SOLUTION TO THE PROBLEM OF WEAK PASSWORDS - PASSWORD QUALITY ASSURANCE USING ENTERPRISE PASSWORD ASSESSMENT SOLUTION (EPAS)

The easiest and fastest way to secure user authentication is to stay with passwords but implement quality assurance measures by strengthening the actual passwords against attack methods.

Detack, an independent provider of high-end IT security services and solutions, has been conducting security audits and penetration testing for 20 years. Through their experience in that role, they have developed a unique, "automated" solution for password quality assurance, Enterprise Password Assessment Solution (EPAS).

Based on patented technology, EPAS regularly audits passwords and passphrases across the enterprise, detecting weak and/or compromised passwords, and assigns a numeric value or "Strength Score" (out of 100) based on how "at risk" each password is to an actual attack.

The password algorithms assess all passwords individually against known weaknesses including:

- **A Dictionary Wordlist-** EPAS compares all passwords against a massive repository wordlist for commonality
- **A Dynamic Wordlist-** a company-specific wordlist created for every instance of EPAS aimed at removing company/application specific password use.
- **Leaked Passwords-** EPAS compares against all known compromised password lists (currently a 1.6TB repository)
- **Shared and Re-Used Passwords-** EPAS checks for re-used and shared passwords across accounts and applications within the business and compares changed passwords against previous versions.
- **Derivations of all Wordlists-** EPAS checks for all d3r1v4t10n$ of all lists above preventing users from making simple adjustments to previous passwords or to recognised dictionary words.
- **Easily Guessed or Derived Passwords-** EPAS tests for structurally weak passwords including passwords that can be easily guessed.
- **Missing and Default Passwords-** EPAS checks across attached devices and admin accounts to find accounts still set with the default passwords or any accounts with no set password.

Each password strength score is compared against the minimum requirement, set by the administrator (by application), and reports are generated that explain the root cause behind the scores applied.

Each assessment delivers a separate compliance report, measuring password quality KPIs, with detailed analysis

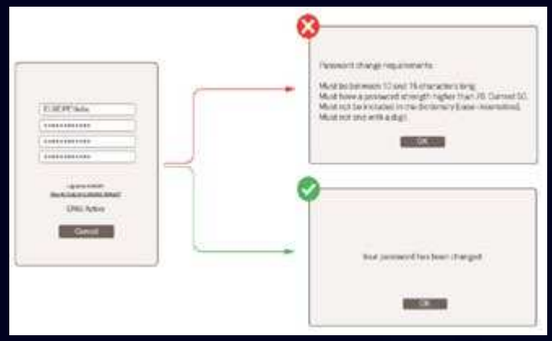

Table 2: Example enforcement feedback to user at login

for all management layers while multiple assessments can be conducted ad-hoc or set to run automatically at set intervals.

Analytics and reporting help to guide teams through planning, implementing, and measuring remediation programs, as well as demonstrating the ongoing improvements in password strength.

Passwords are never stored, just measured, then discarded, so remediation can be achieved without revealing the clear text passwords- maintaining GDPR compliance and reducing insider-threat risks. For the first time, the technology available to attackers is now available and permitted to be used by the good guys.

The optional EPAS Enforcer add-on ensures password integrity is quickly attained and maintained across the business- an outcome not available through any other solution in the market. Following any audit of an application, any "Failed" passwords are quarantined so that when the user next signs in, they are forced to correct and strengthen their password before progressing to the application (see Table 2). Additionally, when users are prompted to update their passwords, or when they sign-in to an application for the first time, the module ensures they create a strong password at that point before they can progress to the application.

The ability to enforce stronger passwords across the enterprise, without compromising the passwords themselves, is what stands EPAS apart from other solutions in the market today.[12]

Launched in 2013, EPAS is currently deployed across thousands of production systems, assessing millions of passwords on a regular, automated basis, with zero impact on system availability.

Detack offers their proven and patented EPAS solution in a simplified, cost-effective, on-premise model. Deployable within 3 to 5 days, EPAS is largely automated and requires minimal resourcing to operate.

PROMOTIONAL OFFER

We are so confident in the solution we are offering a free of charge "Proof of Concept" to any organisation that mentions this advertorial. Our technicians will work with your team to deploy EPAS in your current environment and deliver a baseline report of your password quality. The results speak for themselves. If you would like to explore EPAS in more detail, please reach out to our ANZ representatives at www.whynotconsulting.tech or via email: hello@whynotconsulting.tech

1. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/#comparison-of-top-five-industry-sectors
2. https://www.cyber.gov.au/threats/advisory-2020-009-advanced-persistent-threat-apt-actors-targeting-australian-health-sector-organisations-and-covid-19-essential-services
3. *https://blog.lastpass.com/2019/05/passwords-still-problem-according-2019-verizon-data-breach-investigations-report.html/*
4. *https://enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf*
5. https://australiancybersecuritymagazine.com.au/lastpass-psychology-of-passwords-report-reveals-90-of-australians-know-password-reuse-is-insecure-yet-two-thirds-do-it-any-way/?utm_source=ActiveCampaign&utm_medium=email&utm_content=Psychology+of+Passwords+l+Drones+prove+their+value+l+Threat+Report+plus+latest+news%2C+events%2C+podcasts+and+more&utm_campaign=Thursday+7+May
6. https://thycotic.com/resources/privileged-access-management-maturity-report/?utm_medium=Internal-Email&utm_source=Pardot&utm_campaign=Nurture-Engagement-Flow&utm_content=Prospects&utm_term=Auto_Nurture-Engagement-Flow_Prospects_Email2
7. Enzoic, GDPR Password Policy: Critical Components **https://www.enzoic.com/gdpr-password-policy-critical-components/**
8. Australian Government 2020, Notifiable Data Breaches Report, Office of the Australian Information Commissioner, viewed July 2020, https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2019/AustralianGovernment2020,InformationSecurity Manual, Australian Signals Directorate, viewed June 2020, https://www.cyber.gov.au/acsc/view-all-content/ism)
9. https://www.netsec.news/gdpr-password-policy/
10. Gartner 2020, Gartner Research: Don't Waste Time and Energy Tinkering With Password Policies; Invest in More Robust Authentication Methods or Other Compensating Controls, Gartner, Viewed July 2020, https://www.gartner.com/en/documents/3773163/don-t-waste-time-and-energy-tinkering-with-password-poli
11. Gartner 2020, Peer Insights Review, Gartner, Viewed July 2020, https://www.gartner.com/reviews/market/security-solutions-others/vendor/detack/product/epas