The End of Credential Vulnerabilities: Multi-Layer Dynamic Access Encryption Security as the New Paradigm in Cybersecurity

O Fim das Vulnerabilidades de Credenciais: Segurança de Criptografia de Acesso Dinâmico em Múltiplas Camadas como o Novo Paradigma em Cibersegurança

Julia O'Toole
Co-CEO of MyCena® Security Solutions
julia@mycena.co

ÍNDICE

ABSTRACT

The rapid advancement of artificial intelligence has exposed critical vulnerabilities in traditional identity-based security models. These systems—including MFA, IAM, PAM, and SSO—fundamentally confuse identification (who users are) with authentication (whether they should have access), creating exploitable security gaps as AI-powered attacks increasingly target human-managed credentials as a single point of failure. This research analyzes these limitations and introduces Multi-Layer Dynamic Access Encryption Security (ML-DAES) as an alternative approach.

Through analysis of breach data, expert assessments, and industry reports, this study examines MyCena's ML-DAES as a case study in encryption-based authentication. The methodology evaluates this approach using mathematical combinatorics principles and practical implementation scenarios, focusing on how ML-DAES addresses current vulnerabilities through credentials never seen or managed by humans. This approach creates a security model resistant to phishing, credential stuffing, and deepfake-based social engineering.

The research concludes that ML-DAES transforms cybersecurity by eliminating human error from credential management, effectively neutralizing AI-powered attacks, automating regulatory compliance processes, and significantly reducing operational IT burdens. By properly addressing the identification-authentication gap through encrypted, segmented credentials, organizations can build robust, future-proof defenses that protect critical systems while enhancing operational efficiency in an era of increasingly sophisticated digital threats.

Keywords:
ML-DAES (Multi-Layer Dynamic Access Encryption Security) ; Encryption-based authentication ; AI-driven cyber threats ; Identity-based security ; Mathematical combinatorics

RESUMO

O rápido avanço da inteligência artificial expôs vulnerabilidades críticas nos modelos tradicionais de segurança baseados em identidade. Esses sistemas — incluindo MFA, IAM, PAM e SSO — confundem fundamentalmente identificação (quem são os usuários) com autenticação (se eles devem ter acesso), criando lacunas de segurança exploráveis, à medida que os ataques baseados em IA cada vez mais visam credenciais gerenciadas por humanos como um único ponto de falha. Esta pesquisa analisa essas limitações e apresenta o Multi-Layer Dynamic Access Encryption Security (ML-DAES) como uma abordagem alternativa.

Por meio da análise de dados de violações, avaliações de especialistas e relatórios do setor, este estudo examina o ML-DAES da MyCena como um estudo de caso em autenticação baseada em criptografia. A metodologia avalia essa abordagem utilizando princípios de combinatória matemática e cenários práticos de implementação, com foco em como o ML-DAES aborda as vulnerabilidades atuais por meio de credenciais nunca vistas ou gerenciadas por humanos. Essa abordagem cria um modelo de segurança resistente a ataques de phishing, stuffing de credenciais e engenharia social baseada em deepfakes.

A pesquisa conclui que o ML-DAES transforma a cibersegurança ao eliminar o erro humano na gestão de credenciais, neutralizando efetivamente os ataques baseados em IA, automatizando processos de conformidade regulatória e reduzindo significativamente as cargas operacionais de TI. Ao abordar adequadamente a lacuna entre identificação e autenticação por meio de credenciais criptografadas e segmentadas, as organizações podem construir defesas robustas e preparadas para o futuro, protegendo sistemas críticos e aumentando a eficiência operacional em uma era de ameaças digitais cada vez mais sofisticadas.

Palavras-chave: ML-DAES (Segurança de Criptografia de Acesso Dinâmico em Múltiplas Camadas); Autenticação baseada em criptografia; Ameaças cibernéticas impulsionadas por IA; Segurança baseada em identidade; Combinatória matemática.

INTRODUÇÃO: O PONTO DE INFLEXÃO CRÍTICO NA SEGURANÇA CIBERNÉTICA

A rápida evolução da inteligência artificial (IA) transformou o cenário digital, oferecendo oportunidades sem precedentes e expondo vulnerabilidades críticas de segurança. Os modelos tradicionais de segurança cibernética – MFA, IAM, PAM e SSO – têm uma falha fundamental: eles se concentram em verificar quem são os usuários (identificação) em vez de se eles realmente devem ter acesso (autenticação). Essa confusão histórica cria fraquezas sistêmicas que tecnologias sofisticadas de IA agora exploram por meio de ataques automatizados.

Este artigo apresenta a Segurança de Criptografia de Acesso Dinâmico Multicamada (ML-DAES) da MyCena como uma mudança revolucionária da autenticação baseada em identidade para a autenticação baseada em criptografia. Ao eliminar credenciais gerenciadas por humanos e alavancar a combinatória matemática, o ML-DAES fornece uma defesa à prova de futuro contra ameaças cibernéticas alimentadas por IA oferecendo segurança aprimorada, conformidade regulatória simplificada e eficiência operacional aprimorada para organizações que navegam na era digital.

1. A OBSOLESCÊNCIA DOS MODELOS DE SEGURANÇA BASEADOS EM IDENTIDADE

O aumento das ameaças cibernéticas orientadas por IA expôs uma falha crítica nos modelos de segurança tradicionais: a confusão entre identificação (quem você é) e autenticação (se você deve ter acesso). Esta seção explora como esse equívoco histórico criou vulnerabilidades sistêmicas, levando à obsolescência dos métodos de segurança baseados em identidade no cenário digital atual.

1. O equívoco histórico

Durante décadas, o setor de segurança cibernética operou sob um equívoco fundamental: tratar a identificação e a autenticação como iguais. A principal diferença é que a identificação confirma quem você é, enquanto a autenticação verifica se você tem o direito de acessar recursos específicos.

O objetivo da identificação é verificar quem você é. É mais bem expresso pela **equação de identificação:**

$$I = f(U, A)$$

Onde:

1. I = Resultado de identificação (Verdadeiro/Falso)
2. U = Informações de identidade do usuário (por exemplo, nome de usuário, biometria)
3. A = Banco de dados de autenticação (por exemplo, registros de identidade armazenados)
4. f = Função que compara a identidade fornecida com os registros conhecidos UA

Exemplo: Quando você apresenta sua carteira de identidade, por exemplo, na borda, ou ao fazer um exame, alguém de um sistema verifica se sua identidade apresentada corresponde a um registro no banco de dados.

A identificação verifica a unicidade do usuário:

$$I = U$$

Onde:

1. I = Credencial de identificação (por exemplo, um nome de usuário ou identidade biométrica)
2. U = Identidade do usuário

Isso implica que a mesma identidade é usada para acessar todos os sistemas (One$U$ Identity for All Access), o que cria um único ponto de falha se comprometido. Na **identificação**, uma única identidade comprometida compromete todo o acesso.

O objetivo da autenticação é verificar se você deve ter acesso a um recurso específico. É melhor expresso pela **equação de autenticação**:

$$A = f(K, R)$$

Onde:

1. A = Resultado da autenticação (Acesso concedido/negado)
2. K = Posse da chave ou credencial correta (por exemplo, senha, token de acesso)
3. R = Credencial necessária para o recurso
4. f = Função que verifica se a chave corresponde à credencial necessária KR

Exemplo: Ao entrar em sua casa, a fechadura apenas verifica se a chave se encaixa. Não importa **quem** você é, apenas que você tenha a chave correta.

Você pode ter 10.000 chaves para 10.000 portas, e o sistema só concederá acesso à porta certa com a chave certa.

A autenticação que requer várias chaves para acesso pode ser gravada:

$$A = \sum_{i=1}^{n} Ki$$

Onde:

1. A = Autenticação (direitos de acesso)
2. Ki = Chaves individuais para cada sistema ou ponto de acesso específico
3. n = 10.000 (para 10.000 pontos de acesso exclusivos)

Essa equação mostra que a autenticação não está vinculada a uma única identidade, mas sim a uma coleção de chaves exclusivas. Cada chave é específica para um sistema ou serviço, aumentando a segurança ao garantir que, mesmo que uma chave seja comprometida, ela não afete o acesso a outros sistemas. Na **autenticação**, mesmo que uma chave seja comprometida, o restante dos pontos de acesso permanece seguro.Ki

1. O único ponto de falha: a lacuna de identificação-autenticação

A segurança cibernética sofre com a confusão de identificação com autenticação. A identificação verifica "quem você é", enquanto a autenticação determina "se você deve ter acesso". O arquiteto fundador da Internet, Dr. David Clark, enfatizou em 1988 que essas funções deveriam permanecer separadas. No entanto, a segurança de senha que surgiu na década de 1960 misturou esses conceitos, criando as vulnerabilidades de hoje.

Sistemas de segurança baseados em identidade, como MFA, IAM, PAM e SSO, verificam a identidade do usuário, mas validam inadequadamente os direitos de acesso. Isso cria uma lacuna de identificação e autenticação onde ocorre a maioria dos ataques cibernéticos.

Para ilustrar essa lacuna, imagine começar um novo emprego em que você é solicitado a fazer sua própria chave que abre todas as portas do prédio - desde a entrada até o escritório do CEO e a sala do servidor. Se essa chave fosse perdida ou copiada, qualquer pessoa poderia acessar todas as áreas críticas. Isso reflete como funciona a segurança baseada

em identidade digital, em que um único conjunto de credenciais pode fornecer acesso a uma rede inteira.

O comportamento humano piora esse problema. De acordo com um relatório da Security Magazine de 2022, 78% das pessoas reutilizam senhas em vários sistemas, muitas vezes misturando contas pessoais e profissionais. Isso significa que uma violação em um sistema pode dar aos invasores acesso a muitos outros, multiplicando o risco de infiltração na rede.

Essas credenciais gerenciadas por humanos (senhas, biometria, tokens) criam um único ponto de falha. Quando os invasores comprometem uma identidade, eles geralmente obtêm amplo acesso à rede. A violação do MOVEit de 2023 mostrou como uma vulnerabilidade de terceiros levou a milhares de infiltrações no sistema, pois uma única credencial comprometida se transformou em violações generalizadas.

Ao se concentrar apenas na verificação de identidade, a segurança tradicional cria uma "armadilha de identidade" em que as credenciais roubadas concedem aos invasores acesso a sistemas críticos. O Relatório de Investigações de Violação de Dados da Verizon de 2023 descobriu que 86% das violações de dados envolvem credenciais roubadas, enquanto o Ponemon Institute relatou que 78% das organizações sofreram violações devido a ações internas.

Essa lacuna se torna mais perigosa com vários fornecedores terceirizados. O ataque à SolarWinds em 2020 demonstrou como uma credencial de fornecedor comprometida se tornou um ponto de entrada em vários sistemas governamentais e corporativos, destacando como os modelos de segurança baseados em identidade não conseguem lidar efetivamente com a autenticação, deixando as organizações vulneráveis a ameaças avançadas.

1. O papel da IA na exploração da lacuna de identificação e autenticação

A IA intensificou as vulnerabilidades de segurança automatizando ataques de credenciais e criando identidades sintéticas. Essas ferramentas de IA podem lançar milhares de ataques por segundo, produzir deepfakes convincentes e contornar a segurança explorando padrões de comportamento. De acordo com uma pesquisa da Capgemini de 2024, 97% das organizações sofreram violações de segurança relacionadas à IA generativa no ano passado.

Os invasores usam IA para criar identidades sintéticas que podem derrotar sistemas de verificação sofisticados. Combinadas com credenciais roubadas, essas identidades falsas permitem que os criminosos se movam pelos sistemas enquanto parecem legítimos. O secretário-geral da INTERPOL, Jürgen Stock, descreveu isso como "uma nova dimensão de ataques" em que a IA permite phishing, deepfakes e engenharia social em escala industrial.

A ameaça se estende além do roubo de dados para o controle de operações críticas. À medida que a IA gerencia transações financeiras, cadeias de suprimentos, dispositivos de saúde e infraestrutura, os invasores que comprometem esses sistemas podem manipular as operações, interrompendo sistemas, redirecionando a logística ou alterando transações financeiras.

O envenenamento de dados apresenta outra ameaça séria. Ao contrário dos ataques tradicionais, o envenenamento corrompe os dados de treinamento de IA, afetando a tomada de decisões em seu núcleo. Em um caso, os invasores alteraram os dados de treinamento de um sistema de avaliação de risco financeiro de IA, fazendo com que ele subestimasse os riscos de fraude. O relatório do Belfer Center observa que corromper os dados de treinamento da IA permite que os invasores controlem os resultados.

As apostas são extremamente altas, pois a IA agora gerencia sistemas de saúde, infraestrutura e segurança nacional. Os atores patrocinados pelo Estado visam cada vez mais esses sistemas para prejudicar empresas e economias. As ameaças internas agravam esse risco quando funcionários confiáveis com acesso ao sistema são comprometidos.

O phishing com inteligência artificial tornou-se particularmente perigoso. Esses ataques usam IA para criar campanhas de phishing altamente personalizadas em escala. Nos últimos meses, houve um aumento nos ataques de voz deepfake, em que vozes executivas geradas por IA convencem os funcionários a transferir fundos ou compartilhar informações confidenciais. A CISA relata que 90% dos ataques cibernéticos bem-sucedidos começam com phishing, mostrando que a vulnerabilidade humana continua sendo o principal ponto de entrada.

O rápido crescimento dos serviços de IA criou outra vulnerabilidade por meio de APIs. À medida que as empresas implantam rapidamente a IA por meio de serviços em nuvem, APIs mal protegidas se tornaram os principais alvos. Em 2024, APIs de serviço de IA mal configuradas expuseram mais de 50 milhões de registros confidenciais de clientes em várias empresas da Fortune 500. O mais preocupante é que essas violações ocorreram por meio de simples roubo de credenciais, em vez de explorações técnicas complexas.

As "Diretrizes para o Desenvolvimento Seguro de Sistemas de IA" da CISA identificam vários problemas críticos: APIs configuradas incorretamente, cadeias de suprimentos complexas de IA com vários provedores de serviços e riscos de modelos de IA de terceiros. Cada dependência externa apresenta possíveis falhas de segurança.

À medida que a IA assume papéis mais críticos nas organizações, o dano potencial das violações cresce exponencialmente. Proteger o acesso a sistemas de IA e suas APIs de conexão agora é essencial para proteger os dados e as operações de negócios.

1. APRESENTANDO O ML-DAES: UM NOVO PADRÃO EM SEGURANÇA DE ACESSO

À medida que os modelos tradicionais de segurança baseados em identidade falham contra ameaças orientadas por IA, o Multi-Layer Dynamic Access Encryption Security (ML-DAES) da MyCena oferece uma abordagem transformadora. Esta seção explora como o ML-DAES muda da verificação de identidade para a autenticação baseada em criptografia, aproveitando princípios matemáticos avançados para criar uma barreira de segurança inquebrável.

1. Autenticação baseada em criptografia: uma mudança de paradigma

O ML-DAES apresenta uma transição revolucionária da segurança tradicional baseada em identidade para a autenticação baseada em criptografia. Ao contrário dos sistemas convencionais que validam o acesso confirmando quem são os usuários, o ML-DAES se concentra em saber se os usuários realmente possuem o direito de acessar recursos específicos por meio de credenciais criptografadas geradas dinamicamente que nunca são vistas, compartilhadas ou gerenciadas por humanos.

Essa abordagem elimina o único ponto de falha inerente aos sistemas que dependem de credenciais gerenciadas por humanos. Em vez de armazenar senhas ou tokens de identidade que podem ser roubados ou replicados, o ML-DAES usa chaves geradas criptograficamente e fortemente vinculadas a aplicativos e ambientes específicos. Mesmo que uma credencial seja comprometida, ela não pode ser reutilizada fora do contexto pretendido, impedindo o movimento lateral dentro das redes e minimizando os riscos de violação em larga escala.

1. Combinatória Matemática para Segurança Inquebrável

No núcleo do ML-DAES está a poderosa aplicação da combinatória matemática. Essa abordagem avançada gera credenciais exclusivas e não reproduzíveis usando um modelo de criptografia multicamada. Cada camada de criptografia é aleatória e segmentada de forma independente, garantindo que, mesmo que os invasores violem uma camada, eles não possam decifrar toda a cadeia de credenciais.

A combinatória matemática oferece dois benefícios críticos: tornar os ataques de força bruta virtualmente impossíveis e impedir a replicação de credenciais por meio da geração de identidade sintética ou ataques orientados por IA. Enquanto os sistemas tradicionais que dependem de senhas, biometria ou padrões de comportamento podem ser submetidos a engenharia reversa ou forjados, as credenciais ML-DAES são criadas dinamicamente pelo próprio sistema, sem envolvimento humano na geração, distribuição ou gerenciamento.

Essa abordagem se alinha com a filosofia de design original da Internet, que defendia a manutenção de uma distinção clara entre identificação e autenticação. Ao incorporar complexidade matemática ao processo de autenticação, o ML-DAES cria uma camada de segurança que as tecnologias orientadas por IA não podem violar.

1. Eliminando o elemento humano

A inovação mais significativa do ML-DAES é a eliminação completa das credenciais gerenciadas por humanos. Os sistemas de segurança tradicionais exigem que os usuários criem, gerenciem e insiram credenciais manualmente, introduzindo erro humano e ameaças internas – uma vulnerabilidade bem conhecida destacada por pesquisas que mostram que 78% das violações envolvem ações internas negligentes ou maliciosas.

O ML-DAES remove essa vulnerabilidade automatizando todo o ciclo de vida da credencial. As credenciais são geradas e criptografadas automaticamente, nunca expostas aos usuários e nunca armazenadas de uma forma que possa ser interceptada. Quando o acesso é necessário, o sistema valida a posse da chave criptografada em vez de verificar a identidade do usuário. Esse método simplifica a experiência do usuário, eliminando a necessidade de

senhas e códigos de autenticação multifator, criando um modelo de segurança impermeável a phishing ou engenharia social.

Ao remover o elemento humano da equação, o ML-DAES fecha efetivamente a lacuna que a maioria dos ataques cibernéticos modernos explora. Ele fornece um modelo de segurança robusto e resistente a IA que define um novo padrão de controle de acesso, garantindo que apenas usuários legítimos possam acessar sistemas e dados críticos.

3. IMPACTO NO MUNDO REAL: ML-DAES EM AÇÃO

O ML-DAES demonstra uma eficácia poderosa contra ameaças cibernéticas orientadas por IA, aprimorando os processos de conformidade e transformando as operações de TI. Esta seção explora como o modelo de autenticação avançada do MyCena evita ataques, automatiza a conformidade e reduz a carga de trabalho de TI para fornecer uma solução de segurança robusta e eficiente.

3.1. Parando ataques com inteligência artificial

A vantagem mais significativa do ML-DAES é sua capacidade de neutralizar ataques cibernéticos alimentados por IA. Ao contrário dos métodos tradicionais de segurança baseados em identidade, o ML-DAES emprega autenticação baseada em criptografia que torna os ataques baseados em credenciais ineficazes. Como as credenciais do ML-DAES são geradas dinamicamente, criptografadas e nunca vistas ou compartilhadas por humanos, os invasores não têm nada para roubar ou usar indevidamente.

Os ataques de phishing falham porque os usuários não possuem credenciais para expor. O preenchimento de credenciais se torna inútil porque as credenciais ML-DAES são específicas do aplicativo e não podem ser reutilizadas em sistemas diferentes. Essa abordagem também impede o movimento lateral dentro das redes, uma tática comum em ataques de ransomware em que os invasores aumentam os privilégios usando credenciais roubadas.

A tecnologia cria efetivamente um bloqueio digital nos pontos de acesso, garantindo que, mesmo que os invasores violem uma camada de rede, eles não possam prosseguir. Essa abordagem segmentada minimiza a superfície de ataque, impossibilitando que os cibercriminosos explorem vulnerabilidades de credenciais em escala, uma vantagem crítica à medida que os ataques orientados por IA se tornam cada vez mais sofisticados.

3.2. Racionalização dos esforços de conformidade

A conformidade com regulamentos como GDPR, LGPD, DORA, HIPAA e ISO 27001 requer padrões rigorosos de controle de acesso e proteção de dados. Os métodos tradicionais geralmente envolvem processos manuais para gerar relatórios de conformidade, consumindo tempo e recursos valiosos, com lacunas que podem levar a penalidades de não conformidade.

O ML-DAES automatiza esse processo, fornecendo ferramentas de gerenciamento de acesso e relatórios em tempo real que se alinham aos requisitos regulatórios. O sistema gera logs e relatórios automatizados que demonstram a conformidade com os protocolos de controle de acesso, reduzindo significativamente a carga administrativa. Esses relatórios automatizados são consistentemente precisos e atualizados, permitindo que as organizações adotem uma abordagem proativa para a adesão à regulamentação.

Ao integrar-se perfeitamente à infraestrutura existente, incluindo sistemas IAM, PAM e SSO, o ML-DAES adiciona garantia de conformidade sem revisões disruptivas do sistema. Essa automação ajuda as organizações a evitar multas relacionadas à conformidade, mantendo relacionamentos confiáveis com órgãos reguladores e partes interessadas.

1. Transformando as operações de TI

As equipes de TI geralmente ficam sobrecarregadas com tarefas operacionais, principalmente gerenciamento de senhas e administração de MFA. Uma pesquisa do Ponemon Institute mostra que 40% das chamadas de suporte técnico são relacionadas a senhas, com os funcionários gastando uma média de 11 horas por ano lidando com problemas de senha – tempo que poderia ser gasto em iniciativas estratégicas.

O ML-DAES elimina esses desafios automatizando o gerenciamento de credenciais e removendo totalmente as senhas. Sem senhas para redefinir ou gerenciar, as chamadas de suporte técnico relacionadas a problemas de acesso despencam, liberando a equipe de TI para se concentrar em projetos de crescimento de negócios. Ao eliminar a fadiga da MFA, o ML-DAES também melhora a experiência e a produtividade do usuário, criando eficiências operacionais em toda a organização.

Essa abordagem simplificada reduz o erro humano, um fator significativo nas violações relacionadas a credenciais. Ao remover processos manuais e automatizar o controle de acesso, o ML-DAES transforma as operações de TI de suporte reativo em uma função estratégica proativa, aumentando a agilidade organizacional e a resiliência contra ameaças digitais em evolução.

CONCLUSÃO: UMA MUDANÇA DE PARADIGMA NA ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA

A segurança tradicional baseada em identidade (MFA, IAM, PAM, SSO) não pode mais proteger adequadamente contra ameaças orientadas por IA em evolução. A confusão histórica entre identificação e autenticação criou vulnerabilidades exploráveis por meio de phishing, preenchimento de credenciais e engenharia social deepfake, todas visando credenciais gerenciadas por humanos como um único ponto de falha.

O Multi-Layer Dynamic Access Encryption Security (ML-DAES) da MyCena transforma a segurança cibernética ao:

1. Implementando a autenticação baseada em criptografia
2. Geração de credenciais criptografadas e segmentadas nunca vistas ou compartilhadas por humanos
3. Eliminando riscos de erro humano e roubo de credenciais

4. Simplificando a conformidade regulatória
5. Aumentando a eficiência por meio da redução da carga de trabalho de TI e do gerenciamento automatizado de acesso

No cenário atual de ameaças digitais automatizadas e sofisticadas, a adoção do ML-DAES é essencial. Ao abordar adequadamente a lacuna de identificação-autenticação, as organizações podem criar defesas robustas que protegem sistemas críticos, garantem a conformidade e apoiam a resiliência dos negócios na era da IA.

REFERÊNCIAS

Livros:

- ANDERSON, R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Cambridge: Cambridge University, 2020. Disponível em: https://www.cl.cam.ac.uk/archive/rja14/book.html. Acesso em: 03 mar. 2025.

Relatórios e trabalhos de pesquisa:

- BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS. Attacking AI: How Adversaries Can Disrupt AI Systems. Harvard Kennedy School, 2024. Disponível em: https://www.belfercenter.org/publication/AttackingAI. Acesso em: 03 mar. 2025.
- CAPGEMINI RESEARCH INSTITUTE. New defenses, new threats: What AI and Gen AI bring to cybersecurity. 2024. Disponível em: https://www.capgemini.com/insights/research-library/generative-ai-in-cybersecurity. Acesso em: 03 mar. 2025.
- CENTER FOR SECURITY AND EMERGING TECHNOLOGY (CSET - GEORGETOWN UNIVERSITY). AI Cyber Warfare and Threat Modeling. CSET AI Security Reports, 2024. Disponível em: https://www.cset.georgetown.edu. Acesso em: 03 mar. 2025.
- CLARK, D. D. The Design of the DARPA Internet Protocols. 1988. Disponível em: https://web.mit.edu/6.033/www/papers/darpa.pdf. Acesso em: 03 mar. 2025.
- CYBERINT. Europe Threat Landscape Report. 2024. Disponível em: https://cyberint.com/blog/research/europe-threat-landscape-report/. Acesso em: 03 mar. 2025.
- CYBERPEACE INSTITUTE. Investigating AI-Enabled Cybercrime and Misinformation. 2024. Disponível em: https://www.cyberpeaceinstitute.org. Acesso em: 03 mar. 2025.
- CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA). Secure by Design. 2023. Disponível em: https://www.cisa.gov/sites/default/files/2023-10/SecureByDesign_1025_508c.pdf. Acesso em: 03 mar. 2025.

Artigos e publicações online:

- CORNELL UNIVERSITY. Am I a Real or Fake Celebrity? Measuring Commercial Face Recognition Web APIs under Deepfake Impersonation Attack. Tariq, S., Jeon, S., & Woo, S. S. 2021. Disponível em: https://arxiv.org/abs/2103.00847. Acesso em: 03 mar. 2025.

- CYBERSECURITY DIVE. Your Business Is Connected, and So Is Every Breach. 2024. Disponível em: https://www.cybersecuritydive.com/news/connected-breached-third-party/641857. Acesso em: 03 mar. 2025.
- FORBES ADVISOR. American Password Habits: Statistics and Trends. 2023. Disponível em: https://www.forbes.com/advisor/business/software/american-password-habits/. Acesso em: 03 mar. 2025.
- GOOGLE & HARRIS POLL. Google Security Infographic: Online Password and Security Habits. 2019. Disponível em: https://services.google.com/fh/files/blogs/google_security_infographic.pdf. Acesso em: 03 mar. 2025.

Relatórios Institucionais:

- DEPARTMENT OF HOMELAND SECURITY (DHS). Increasing Threats of Deepfake Identities. 2021. Disponível em: https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf. Acesso em: 03 mar. 2025.
- EUROPEAN UNION AGENCY FOR CYBERSECURITY (ENISA). AI Threat Landscape Report. 2024. Disponível em: https://www.enisa.europa.eu. Acesso em: 03 mar. 2025.
- GOVERNMENT ACCOUNTABILITY OFFICE (GAO). SolarWinds Cyberattack Demands Significant Federal and Private Sector Response. 2021. Disponível em: https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic. Acesso em: 03 mar. 2025.
- NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). Special Publication 800-63, Revision 3: Digital Identity Guidelines. 2017. Disponível em: https://pages.nist.gov/800-63-3/sp800-63-3.html. Acesso em: 03 mar. 2025.
- ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (OECD). AI Security, Responsible AI Development, and Cyber Policies. 2024. Disponível em: https://www.oecd.org. Acesso em: 03 mar. 2025.

Fontes adicionais:

- SECURITY MAGAZINE. 78% of people use the same password across multiple accounts. Security Magazine, 2022. Disponível em: https://www.securitymagazine.com/articles/100765-78-of-people-use-the-same-password-across-multiple-accounts. Acesso em: 03 mar. 2025.
- VERIZON. 2023 Data Breach Investigations Report. 2023. Disponível em: https://www.verizon.com/about/news/2023-data-breach-investigations-report. Acesso em: 03 mar. 2025.
- WALLARM. API Security Report 2025. 2025. Disponível em: https://www.wallarm.com/reports/2025-api-security-report. Acesso em: 03 mar. 2025.
- WIKIPEDIA. MOVEit Data Breach 2023. 2023. Disponível em: https://en.wikipedia.org/wiki/2023_MOVEit_data_breach. Acesso em: 03 mar. 2025.