정보보호 해외진출 전략거점(동남아) 3월 주요동향

2026. 3. 31(화), 한국인터넷진흥원 AI보안산업본부 AI보안산업단 글로벌협력팀

이슈	주요내용 및 시사점
[인도네시아] 개인정보 유출	▸ **인도네시아 인구 2억4천만 명 데이터가 다크웹에서 판매됐다는 의혹이 제기됐음(3월 2일)** ✓ 소셜미디어 'Threat Watchdog' 계정이 인도네시아 2억4천만 명 데이터 유출 의혹을 제기했음. ✓ YUKA라는 행위자가 데이터를 판매한다는 주장과 darkforums.me 링크가 제시됐으나 현재 접속 불가 상태였음. ✓ PT Vaksincom 전문가 알폰스 타누자야는 해당 주장 신뢰성이 낮고 기존 유출 데이터 재유포 가능성을 언급함. ✓ ICSF(인도네시아 Cyber Security Forum) 회장 아르디 수테드자는 반복되는 유출 의혹에도 정부 대응이 부족했다고 지적함. ✓ 전문가들은 개인정보보호법 PDP(Personal Data Protection) 실효성 점검과 함께 규제 강화 및 디지털 문해력 제고 필요성을 강조함. ✓ https://www.tempo.co/digital/benarkah-data-240-juta-penduduk-인도네시아-dijual-di-dark-web-2118766
[인도네시아] 글로벌 보안기업과의 협력	▸ **인도네시아와 글로벌 방위보안기업 Thales가 Universitas Pertahanan Republik 인도네시아를 통해 협력에 나섰음(3월 2일)** ✓ 사이버보안이 국가 데이터 보호와 방위 체계 강화를 위한 전략적 핵심 분야로 부상하고 있음. ✓ 인도네시아 국방대학교 UNHAN RI(Universitas Pertahanan Republik 인도네시아)는 2026년 2월 Thales와 사이버보안 인재 양성을 위한 협정을 체결했음. ✓ 이번 협약은 안톤 누그로호 총장과 니콜라 부브로 Thales 아시아 부사장이 서명했으며 국방 사이버 역량 강화를 목표로 함. ✓ 국가사이버암호청 BSSN(Badan Siber dan Sandi Negara)에 따르면 2025년 1~7월 동안 36억 건 이상의 사이버 공격이 탐지돼 위협이 심화됨. ✓ UNHAN RI는 석박사 과정 운영과 함께 Thales 협력을 통해 2026년 2분기부터 교육을 시작하며 사이버 주권 강화를 기대함. ✓ https://www.zonajakarta.com/nasional/67316800104/364-miliar-serangan-siber-melanda-인도네시아-thales-prancis-siap-turun-tangan-bantu-atasi-lewat-unhan-ri?page=2

[인도네시아] 인도네시아와 미국간 무역 협정	▸ **인도네시아와 미국 간 무역 협정이 국내 사이버보안 산업에 긍정적 촉매가 될 것으로 평가됨(3월 4일)** ✓ 인도네시아-미국 상호무역협정 ART(인도네시아-United States Reciprocal Trade Agreement/Perjanjian Perdagangan Resiprokal 인도네시아-Amerika Serikat)가 사이버보안 산업 성장의 주요 촉진 요인으로 평가됨. ✓ ITSEC Asia의 패트릭 단나허 CEO는 ART가 디지털 무역 협정 이전 미국과 협의를 요구하며 사이버보안을 핵심 협력 의제로 부상시켰다고 설명함. ✓ 협정은 핵심 인프라 보호와 사이버보안 모범 관행 도입, 양국 간 위협 대응 협력을 촉진함. ✓ 이에 따라 BUMN(State-owned enterprises/Badan Usaha Milik Negara)과 주요 기업들이 더 높은 보안 기준을 채택할 것으로 예상됨. ✓ 전문가들은 2FA(Two-Factor Authentication) 등 보안 강화 조치와 함께 ART가 사이버보안을 필수 요소로 정착시키는 계기가 될 것으로 평가함. ✓ https://www.sultramedia.id/teknologi/mobile/perjanjian-perdagangan-인도네시아-as-katalis-positif-industri-keamanan-siber-nasio
[인도네시아] 통신사 AI위협대응	▸ **통신사 Indosat Ooredoo Hutchison이 AI 위협 대응을 위해 자카르타에 사이버 허브를 개설했음(3월 4일)** ✓ 인도삿 오레두 허치슨 Indosat Ooredoo Hutchison이 자카르타에 SCC(Security Command Centre)를 구축해 관리형 사이버보안 서비스를 시작함. ✓ 해당 센터는 Cisco와 Splunk 기술, Cisco Customer Experience Services 기반으로 실시간 모니터링과 사고 대응 기능을 제공함. ✓ AI 기반 분석과 실시간 탐지·조사·대응 기능을 통해 복잡해지는 사이버 위협 대응을 강화하도록 설계됨. ✓ SCC는 24시간 관리형 보안 서비스로 다양한 조직의 보안 접근성을 확대하는 것을 목표로 함. ✓ SOC(Security Operations Center) 확대 흐름 속에서 인도삿은 이를 디지털 전략 핵심 인프라로 활용하며 국가 사이버 회복력 강화에 기여할 것으로 기대됨. ✓ https://securitybrief.asia/story/indosat-opens-jakarta-cyber-hub-to-counter-ai-threats

[인도네시아] 사이버공격 현황	▸ **인도네시아에서 2025년 하루 평균 4만848건의 사이버 공격 시도가 발생(3월 5일)** ✓ 인도네시아는 AI(Artificial Intelligence) 활용 주요 시장으로 부상했으며 AI 도입 준비 수준이 약 65.85퍼센트에 도달함. ✓ 디지털 전환과 AI 확산과 함께 사이버 범죄도 빠르게 증가하는 추세를 보임. ✓ Kaspersky에 따르면 2025년 약 1,490만 건의 웹 기반 공격이 탐지됐으며 하루 평균 4만 건 이상의 공격 시도가 발생함. ✓ 전체 사용자 중 약 22.4퍼센트가 온라인 위협을 경험했으며 브라우저 취약점과 사회공학 공격이 주요 방식으로 분석됨. ✓ 전문가들은 2FA(Two-Factor Authentication) 등 보안 수칙 준수와 함께 AI가 공격과 방어 양측에 활용될 수 있다고 경고함. ✓ pengovasia.com/the-philippines-national-id-for-smarter-faster-safer-services/?c=globalhttps:/
[인도네시아] AI 사용 규제	▸ **Telkom 인도네시아가 데이터 유출 방지를 위해 AI 사용에 대한 엄격한 규제를 촉구했음(3월 6일)** ✓ 텔콤 인도네시아 Telkom 인도네시아는 ChatGPT, Gemini 등 공개형 AI(Artificial Intelligence) 사용이 기업 데이터 유출 위험을 초래할 수 있다고 경고함. ✓ 코망 부디 아르야사는 업무 문서를 외부 AI 서비스에 업로드할 경우 데이터가 외부 서버에 저장될 수 있다고 설명함. ✓ 이로 인해 유사 질문을 통해 기업 문서가 노출되거나 경쟁사 및 악의적 사용자에게 전달될 위험이 존재함. ✓ AI 활용을 위해서는 기업 차원의 명확한 사용 규정과 경영진 주도의 관리 체계 구축이 필요함. ✓ 기업 내부 인트라넷 기반 GPT 시스템 도입을 통해 데이터 보호와 AI 활용 효율성을 동시에 확보할 수 있다고 제시함. ✓ https://rmol.id/bisnis/read/2026/03/03/699188/telkom-dorong-aturan-tegas-penggunaan-ai-demi-cegah-kebocoran-data

[인도네시아] 글로벌기업의 정보보호 현황 점검	▸ **디지털통신부(Kementerian Komunikasi dan Digital)에서 글로벌기업 Meta 인니 사무실 불시점검에서 사이버보안 위험 신호 감지(3월 6일)** ✓ 인도네시아 디지털통신부 장관 메우티아 하피드가 Meta 인도네시아 사무실을 점검하며 규제 준수 실태를 확인함. ✓ 점검 결과 Meta의 국내 규제 준수 수준이 30퍼센트 이하로 나타나 이용자 보호와 책임성 문제가 제기됨. ✓ 전문가 프라타마 페르사다는 이를 국가 사이버보안에 대한 경고 신호로 평가하며 사기 콘텐츠 확산 가능성을 지적함. ✓ 또한 공격자들이 코드 변형, 이미지 변형, 계정 네트워크 등을 활용해 검열을 회피하고 있다고 분석됨. ✓ BIN(Badan Intelijen Negara), BSSN(Badan Siber dan Sandi Negara) 등 기관이 참여한 가운데 실질적 감독과 법 집행 강화 필요성이 강조됨. ✓ https://www.liputan6.com/tekno/read/6292395/menkomdigi-sidak-meta-pakar-sinyal-bahaya-keamanan-siber-di-인도네시아#google_vignette
[인도네시아] AI 리터러시 확산	▸ **인도네시아는 비판적 사고를 지키면서 AI 리터러시 확산을 추진하고 있음(3월 9일)** ✓ 인도네시아 부통령 기브란 라카부밍 라카가 교사와 학부모의 AI(Artificial Intelligence) 이해도 제고 필요성을 강조함. ✓ 반둥 AI Ready ASEAN 워크숍에서 AI 활용 능력이 전 사회 구성원에게 중요해지고 있다고 언급함. ✓ 교사와 부모가 기술 변화에 대응해 아이들의 올바른 디지털 성장 지도를 해야 한다고 강조함. ✓ AI 활용과 함께 비판적 사고와 책임 있는 사용 능력이 필요하며 과도한 의존은 경계해야 한다고 지적함. ✓ 정부는 국가 AI 로드맵 National Artificial Intelligence Roadmap을 통해 윤리적이고 책임 있는 AI 활용 정책을 제시할 계획임. ✓ https://opengovasia.com/인도네시아-driving-ai-literacy-while-safeguarding-critical-thinking/?c=global

[인도네시아] 사이버 보안 게임 개최	▸ **인도네시아에서 사이버 공격 대비를 위해 국가방위위원회(Dewan Pertahanan Nasional)이 사이버 보안 게임 개최(3월 10일)** ✓ 인도네시아 국가방위위원회 DPN(Dewan Pertahanan Nasional)이 자카르타에서 Cyber Security Admin Game 형태의 사이버 보안 워게임을 개최함. ✓ 사이버 위협의 복잡성과 조직화 증가에 대응하기 위해 국가 차원의 대응 역량 강화를 목표로 함. ✓ 도니 에르마완 타우판토 차관은 사이버 공격이 정치, 경제, 사회, 국방 전반의 안정성을 위협할 수 있다고 강조함. ✓ Information Warfare, Cyber Warfare, Cognitive Warfare, Neocortex Warfare 등 다양한 비물리적 공격이 국가 주권에 영향을 줄 수 있다고 설명함. ✓ DPN은 Komdigi(Kementerian Komunikasi dan Digital) 등 기관이 참여한 가운데 대응 체계 통합과 법·제도 개선 필요성을 강조함. ✓ https://jawapos.com/nasional/2511060390/antisipasi-serangan-siber-ke-인도네시아-dpn-selenggarakan-admin-game-cyber-security
[인도네시아] 아동의 온라인 안전	▸ **디지털통신부가 아동 대상 SNS 이용제한 규정을 발표하며 Tik Tok과 Instagram 등이 영향을 받게 됐음(3월 11일)** ✓ 인도네시아 정부가 16세 미만 아동의 소셜미디어 이용을 제한하는 규정을 발표했으며 2026년 3월 28일부터 시행 예정임. ✓ Komdigi(Kementerian Komunikasi dan Digital)의 메우티아 하피드 장관은 아동 보호와 부모 감독 강화를 위한 조치라고 설명함. ✓ AI(Artificial Intelligence) 알고리즘 영향력 확대에 따라 아동의 디지털 환경 보호를 위한 국가 개입 필요성이 강조됨. ✓ YouTube, TikTok, Facebook, Instagram, X, Roblox 등 주요 플랫폼 이용 제한을 통해 온라인 위험을 줄이는 것이 목적임. ✓ DPRD(Dewan Perwakilan Rakyat Daerah)도 지지를 표명했으며 정부는 공동 책임 기반 협력 체계 구축 필요성을 강조함. ✓ https://radarsurabayabisnis.jawapos.com/industri-perdagangan/2187282868/peraturan-sosmed-untuk-anak-resmi-diterbitkan-tiktok-hingga-instagram-terdampak-berikut-aturannya#goog_rewarded

[인도네시아] 사이버 보안 기본법 추진	▸ **인도네시아 하원이 사이버 보안 및 회복력 법안 관련 대통령 서한을 접수했음(3월 12일)** ✓ 인도네시아 의회 DPR(Dewan Perwakilan Rakyat)이 사이버보안 관련 대통령 서한을 접수하고 입법 논의를 시작할 예정임. ✓ 해당 서한에는 사이버 보안 및 회복력 법안 RUU Keamanan dan Ketahanan Siber가 포함됐으며 국가 차원의 대응 기반 마련을 목표로 함. ✓ Puan Maharani 의장은 이 법안이 증가하는 사이버 위협에 대응하기 위한 것이라고 설명함. ✓ 그러나 시민사회와 연구자들은 군사 중심 접근과 인권 및 시민 자유 침해 가능성을 우려함. ✓ 언론단체들은 해킹, 도싱 등으로부터 기자 보호 장치가 부족할 경우 언론 자유에 부정적 영향을 줄 수 있다고 경고함. ✓ https://www.tempo.co/politik/dpr-terima-surpres-ruu-keamanan-dan-ketahanan-siber-2121508#google_vignette
[인도네시아] 4자협력(Quadruple Helix)모델의 사이버보안	▸ **BSSN이 국가 사이버보안 생태계 강화를 위해** Quadruple Helix 협력 모델**을 추진하고 있음(3월 12일)** ✓ 인도네시아 국가사이버암호청 BSSN(Badan Siber dan Sandi Negara)이 Quadruple Helix 모델을 통해 국가 사이버보안 생태계 강화를 추진함. ✓ 정부, 산업, 학계, 커뮤니티 협력을 기반으로 사이버 회복력이 디지털 전환의 핵심 요소로 강조됨. ✓ CyberTalk 행사에서 언론이 사이버 위협 정보 전달과 인식 확산의 전략적 파트너로 평가됨. ✓ 사이버 위협이 인프라 공격, 악성코드, 허위정보 등 다양한 형태로 복잡해지고 있음. ✓ BSSN은 Cyber Resilience and Defense 2026 포럼 추진과 함께 People, Process, Technology 기반 대응 중요성을 강조함. ✓ https://www.pantau.com/nasional/328844/bssn-dorong-kolaborasi-quad-helix-untuk-perkuat-ekosistem-keamanan-siber-nasional

[인도네시아] AI 데이터센터	▸ **Telkom 인도네시아가 F5와 협력해 AI 데이터센터를 추진함(3월 13일)** ✓ PT Telkom Data Ekosistem NeutraDC가 F5 Inc.와 AI 기반 데이터 센터 연결 기술 개발을 위한 MoU를 체결함. ✓ 이번 협약은 Mobile World Congress 2026 기간 중 바르셀로나에서 체결됨. ✓ NeutraDC 인프라에 F5의 AI 보안 및 애플리케이션 전달 기술을 통합해 AI connectivity 구축을 목표로 함. ✓ 하이브리드 및 멀티클라우드 환경 대응을 위한 데이터센터 및 연결 서비스 역량 강화가 추진됨. ✓ 해당 협력은 Telkom 인도네시아의 AI 기반 디지털 인프라 전략과 국가 디지털 전환 가속화를 위한 일환으로 평가됨. ✓ https://infodigital.co.id/telkom-gandeng-f5-hadirkan-data-center-ai/
[인도네시아] 정부간 데이터 공유	▸ **디지털통신부가 원 데이터 인도네시아 정책 지원을 위해 데이터 공유 절차를 마련하고 있음(3월 13일)** ✓ 고론탈로 주 정부가 DTSEN(Data Tunggal Sosial Ekonomi Nasional) 공동 활용을 위한 업무 프로세스를 마련 중임. ✓ 해당 계획은 Satu Data 인도네시아 정책에 따라 정부 데이터 관리 체계 통합을 지원함. ✓ 지방정부 기관의 데이터 요청, 검증, 활용 과정을 체계적이고 투명하게 운영하는 것이 목표임. ✓ BNBA(By Name By Address) 기반 데이터 관리 도입으로 개인·가구 단위 데이터 정확성을 강화함. ✓ PENTAGON 애플리케이션과 통합 보안 시스템을 통해 민감 정보 접근을 제한하고 정책 활용 효율성을 높임. ✓ https://berita.gorontaloprov.go.id/2026/03/13/dukung-satu-data-인도네시아-kominfo-susun-proses-berbagi-data-dtsen/
[인도네시아] 사이버공간의 글로벌 지정학 경쟁의 무대화	▸ **Universitas 인도네시아 연구는 사이버 공간이 글로벌 지정학 경쟁의 무대가 되고 있다고 밝혔음(3월 13일)** ✓ 인도네시아 연구자들은 사이버 공간이 글로벌 지정학 경쟁의 전략적 전장으로 변화하고 있다고 분석함. ✓ Universitas 인도네시아 알리 압둘라 위비소노 교수는 디지털 의존도 증가로 사이버 공격이 국가 안보에 직접 영향을 미친다고 설명함. ✓ 해당 연구는 사이버 공간을 다섯 번째 전쟁 영역으로 규정하며 사이버 외교와 디지털 안보 전략 필요성을 강조함. ✓ 인도네시아는 법적 프레임워크 부족과 인프라 격차, 미중 기술 경쟁 등 복합적 도전에 직면해 있음. ✓ ICSF(인도네시아 Cyber Security Forum)는 최근 6개월간 약 36억 건의 공격이 발생했다고 밝히며 규제 강화와 국제 협력 필요성을 강조함. ✓ https://megapolitan.antaranews.com/berita/512130/riset-ui-sebut-ruang-siber-jadi-medan-rivalitas-geopolitik-global

[인도네시아] 데이터센터	▸ **Telkom 인도네시아가 Huawei와 협력해 데이터센터와 디지털 인프라를 강화함(3월 16일)** ✓ PT Telkom 인도네시아가 자회사 NeutraDC를 통해 Huawei Technologies Co., Ltd.와 디지털 텔코 및 데이터센터 개발을 위한 MoU를 체결함. ✓ 이번 협약은 Mobile World Congress 2026에서 체결됐으며 디지털 인프라와 데이터센터 생태계 강화를 목표로 함. ✓ NeutraDC는 데이터센터 플랫폼 역할을 맡고 Huawei는 클라우드 availability zone 구축과 기술 협력을 추진함. ✓ Huawei는 MEP 시스템, AI(Artificial Intelligence) 기반 하드웨어, 데이터센터 아키텍처 및 운영 기술 지식 공유를 제공할 예정임. ✓ 양사는 ICT 역량 확대와 AI-ready 인프라 강화를 통해 인도네시아 디지털 경제 경쟁력 제고를 추진함. ✓ https://www.tvonenews.com/berita/nasional/424501-telkom-gandeng-huawei-di-mwc-barcelona-perkuat-data-center-dan-infrastruktur-digital-인도네시아
[인도네시아] 데이터센터	▸ **인도네시아가 지역 데이터센터 허브 도약을 위한 노력을 강화하고 있음(3월 20일)** ✓ 인도네시아가 디지털 경제 성장과 AI·클라우드 수요 증가로 동남아 데이터센터 허브로 부상하고 있음. ✓ 현재 약 200개 데이터센터가 운영 중이며 글로벌 기업과 지역 사업자의 투자가 지속 확대되고 있음. ✓ Microsoft는 서자바 카라왕에 48MW 데이터센터와 5개 시설 클러스터 구축을 추진 중임. ✓ Digital Edge는 브카시에서 500MW 규모 CGK 캠퍼스를 개발하며 시장 입지를 강화하고 있음. ✓ 특구 확대와 규제 개선 필요성이 제기되는 가운데 자원 확보와 인허가 문제 등 과제가 병존함. ✓ https://www.channelnewsasia.com/asia/인도네시아-regional-data-centre-hub-challenges-6003811

[인도네시아] (3월 21일) 데이터센터	▸ **인도네시아가 데이터센터 확대에 나서며 외국인 투자가 급증하고 있음(3월 21일)** ✓ 인도네시아가 디지털 경제 성장과 AI·클라우드 수요 증가로 동남아 데이터센터 허브로 빠르게 부상하고 있음. ✓ 약 200개 데이터센터 운영과 함께 Microsoft, Digital Edge 등 글로벌 기업 투자로 인프라 경쟁이 본격화됨. ✓ 정부는 바탐 농사 디지털 파크 모델을 기반으로 세제 혜택과 규제 완화를 통해 투자 유치를 확대하고 있음. ✓ 자카르타 인근은 토지 부족, 환경 규제, 전력·수자원 문제로 입지와 친환경 기술 도입이 주요 과제로 부상함. ✓ 전문 인력 부족 대응을 위해 산업계와 교육기관 협력을 통한 인재 양성이 중요 과제로 제시됨. ✓ https://www.idnfinancials.com/news/62366/foreign-investment-surges-as-인도네시아-ramps-up-regional-data-centers
[인도네시아] 아동의 온라인 안전	▸ **인도네시아가 아동의 건강한 성장을 위해 스크린 시간과 온라인 안전의 균형을 강조하고 있음(3월 26일)** ✓ 인도네시아 아동보호위원회 KPAI(Komisi Perlindungan Anak 인도네시아)가 온라인 안전 규정의 엄격한 집행을 정부에 촉구함. ✓ 이번 조치는 PP Tunas(Government Regulation No. 17 of 2025)를 중심으로 아동 보호 강화를 위한 정책 흐름 속에서 추진됨. ✓ 플랫폼은 연령 적합 설계, 미성년자 접근 제한, 콘텐츠 모니터링 등 보호 조치를 강화해야 함. ✓ 16세 미만 소셜미디어 제한과 함께 사이버불링 및 유해 콘텐츠 노출 대응 필요성이 강조됨. ✓ 가족 참여와 함께 'One Quality Hour with Family Movement' 등 병행을 통해 아동 디지털 안전과 정서 보호가 중요함. ✓ https://opengovasia.com/인도네시아-balancing-screen-time-and-safety-for-child-well-being/?c=global

[인도네시아] 아동 온라인 안전	▸ **인도네시아가 아동 온라인 보호를 위해 디지털 리터러시와 윤리 교육을 강화하고 있음(3월 30일)** ✓ 인도네시아가 교사 역할 확대와 디지털 리터러시 교육을 통해 아동 보호를 강화하고 있음. ✓ 이 정책은 PP Tunas(Government Regulation No. 17 of 2025) 시행과 연계된 국가 전략의 일환임. ✓ 아동이 허위정보, 사이버불링, 유해 콘텐츠에 노출되는 위험 증가에 따라 교육 현장 역할이 강조됨. ✓ 교사는 기술 교육을 넘어 비판적 사고와 윤리적 판단, 책임 있는 온라인 행동을 지도함. ✓ 전 교과 통합 교육과 교사 역량 강화, 지역사회 협력을 통해 디지털 시민 양성을 목표로 함. ✓ https://opengovasia.com/인도네시아-focus-on-digital-literacy-ethics-to-protect-children-online/?c=global
[싱가포르] 기업 정보 유출	▸ **다크웹 유출 주장으로 싱가포르 내 255개 기업이 표적이 됐다는 우려가 커지고 있음(3월 2일)** ✓ 싱가포르에서 다크웹 유출 자료로 CII(Critical Information Infrastructure) 관련 약 255개 기관이 공격 대상이라는 주장이 제기됨. ✓ 유출 문서 약 1만2천 건에는 통신, 에너지, 금융 분야 침해 주장 내용이 포함됐으나 실제 침해 여부는 확인되지 않음. ✓ 해당 데이터는 보안 기업을 자칭한 단체에서 유래했으며 현재 진위 여부가 조사 중임. ✓ CSA(Cyber Security Agency of 싱가포르)에 따르면 APT(Advanced Persistent Threat) 공격이 크게 증가했고 SME(Small and Medium-sized Enterprises)의 취약성도 확대됨. ✓ 정부는 공급망 보안 강화와 국제 공조를 추진하며 유출 자료의 신뢰성과 실제 침해 가능성을 지속 분석 중임. ✓ https://the420.in/싱가포르-dark-web-leak-255-firms-cybersecurity-cii/

[싱가포르] AI 도입 가속화	▸ **싱가포르가 AI 도입 가속화를 위한 국가 프로그램을 추진하고 있음(3월 3일)** ✓ 싱가포르가 National AI Impact Programme을 출범해 기업 AI 도입과 인력 역량 강화를 추진함. ✓ MDDI(Ministry of Digital Development and Information) 주도로 3년간 최대 1만 개 기업의 AI 통합과 생산성 향상을 지원함. ✓ IMDA(Infocomm Media Development Authority)에 따르면 중소기업과 대기업 모두 AI 활용률이 크게 증가함. ✓ 정부는 10만 명 규모의 AI 이중언어 인재 양성과 기업 리더 교육, PSG(Produtivity Solutions Grant) 지원 확대를 추진함. ✓ 책임 있는 거버넌스와 윤리 기준을 병행해 AI 기반 경제 전환과 경쟁력 확보를 목표로 함. ✓ https://opengovasia.com/싱가포르-national-programme-to-accelerate-ai-adoption/?c=global
[싱가포르] 인프라 위협탐지 등 보호	▸ **싱가포르가 중요 정보 인프라 운영자에게 자체 위협 탐지 시스템 도입을 계획하고 있음(3월 4일)** ✓ 싱가포르 정부가 CIIO(Critical Information Infrastructure Owners)의 사이버 방어 역량 강화를 위해 신규 보안 조치를 도입할 계획임. ✓ 정부 기술을 기반으로 CSIT(Centre for Strategic Infocomm Technologies)가 개발한 위협 탐지 시스템을 CII(Critical Information Infrastructure)에 단계적으로 확대 적용함. ✓ APT(Advanced Persistent Threat) 대응을 위해 민간과 기밀 위협 정보 공유 및 재정 지원도 검토됨. ✓ 이번 조치는 UNC3886 관련 통신사 공격 시도 이후 강화된 대응 전략의 일환임. ✓ CSA(Cyber Security Agency of 싱가포르)는 CTM(Cyber Trust Mark) 의무화와 함께 디지털 기기 보안 기준 강화를 추진함. ✓ https://www.channelnewsasia.com/싱가포르/critical-information-infrastructure-owners-government-proprietary-threat-detection-systems-5963256

[싱가포르] 인프라 위협탐지 등 보호	▸ **싱가포르가 UNC3886 공격 이후 자체 위협 탐지 도구 개발을 추진하고 있음(3월 4일)** ✓ 싱가포르가 APT(Advanced Persistent Threat) 대응을 위해 국가 차원의 위협 탐지 도구를 개발·배포할 계획임. ✓ UNC3886 관련 통신사 공격 이후 사이버 방어 역량 강화를 위한 대응으로 추진됨. ✓ CSA(Cyber Security Agency of 싱가포르)에 따르면 CSIT(Centre for Strategic Infocomm Technologies)가 개발한 기술이 일부 CII(Critical Information Infrastructure)에 적용됨. ✓ 정부는 기밀 위협 정보 공유와 함께 통신사 보안 요구 및 IMDA(Infocomm Media Development Authority) 규제를 강화함. ✓ Cyber Trust Mark 인증 의무화와 디지털 기기 보안 기준 상향을 통해 국가 전반의 방어 체계를 강화함. ✓ https://www.straitstimes.com/싱가포르/politics/싱가포르-develops-its-own-threat-detection-tool-on-the-heels-of-unc3886-attacks
[싱가포르] 가정용 라우터 보안 및 중요 인프라 보안	▸ **싱가포르가 예산 2026에서 가정용 라우터 보안을 강화하고 중요 인프라 보안 기준을 높임(3월 5일)** ✓ 싱가포르가 2027년까지 가정용 라우터의 사이버보안 기준을 강화할 계획임. ✓ CSA(Cyber Security Agency of 싱가포르)와 IMDA(Infocomm Media Development Authority)는 CLS(Cybersecurity Labelling Scheme)를 레벨 2로 상향 적용할 예정임. ✓ 레벨 2는 통신 보안, 데이터 보호, 인증 체계 등 강화된 보안 요구사항을 포함함. ✓ 이번 조치는 수천 대 기기 감염 사건 이후 개인정보 보호와 기기 보안 강화를 위한 대응임. ✓ IPC(Internet Protocol Camera) 등 기기 확대와 함께 CTM(Cyber Trust Mark) 최고 등급 의무화를 통해 국가 보안 수준을 높임. ✓ https://www.businesstimes.com.sg/싱가포르/budget-2026-싱가포르-mandates-stricter-security-home-routers-raises-bar-critical-infrastructure

[싱가포르] 사이버보안 우려사항	▸ **사이버보안 책임자의 약 87%가 개인적 법적 책임 위험을 우려하고 있음(3월 5일)** ✓ 싱가포르 CISO(Chief Information Security Officer)의 약 87퍼센트가 사이버 사고 시 개인적 법적 책임을 우려함. ✓ 응답자의 85.7퍼센트는 역할 복잡성과 업무 부담이 크게 증가했다고 답함. ✓ CSA(Cyber Security Agency of 싱가포르) 등 당국은 사이버보안을 경영진 차원의 책임으로 강조함. ✓ CISO는 DevSecOps(Development, Security and Operations), 공급망 보안, AI 거버넌스 등 다양한 영역을 동시에 관리함. ✓ MTTD(Mean Time to Detect), MTTR(Mean Time to Respond) 지표 활용과 함께 조직 전반의 공동 책임과 데이터 가시성 확보 중요성이 강조됨. ✓ https://sbr.com.sg/information-technology/news/about-87-cyber security-leaders-fear-personal-liability-risks
[싱가포르] 사이버 위협 대응 부문 회복력 국가순위	▸ **싱가포르가 사이버 위협 대응 부문 회복력에서 세계 2위를 기록했음(3월 10일)** ✓ 싱가포르가 WiredScore 보고서에서 건물 디지털 인프라 회복력 세계 2위를 기록함. ✓ 상업용 건물의 냉방, 조명, 출입 통제 시스템 등 디지털 운영 인프라가 새로운 사이버 공격 표적으로 부상함. ✓ 국가 광섬유 네트워크와 IMDA(Infocomm Media Development Authority) 표준 기반 스마트 건물 운영이 이루어지고 있음. ✓ 그러나 약 75퍼센트 조직이 취약한 건물 관리 시스템을 보유하고 OT(Operational Technology) 관련 사고 비중도 높은 것으로 나타남. ✓ AI(Artificial Intelligence)와 자동화 확산으로 건물 운영 마비 위험이 커지고 있어 보안 대응 필요성이 강조됨. ✓ https://sbr.com.sg/news/싱가포르-ranks-2nd-in-real-estate-resilience-against-cyber-threats
[싱가포르] 양자컴퓨팅 관련 대응	▸ **싱가포르가 양자 인재 양성과 연구 인프라 강화를 추진하고 있음(3월 13일)** ✓ 싱가포르가 양자 컴퓨팅 R&D 센터를 출범하며 글로벌 양자 기술 경쟁에서 입지를 강화함. ✓ 해당 센터는 연구, 인재 양성, 산업 협력을 통해 기술 개발과 상용화를 가속화하는 것을 목표로 함. ✓ 싱가포르는 반도체 생산과 장비 분야에서 주요 제조 허브로 성장했으며 양자 연구도 지속 확대해옴. ✓ National Quantum Strategy를 통해 대규모 투자와 함께 연구 프로그램과 스타트업 생태계를 육성함. ✓ Helios-2 시스템 도입과 함께 금융, 물류, 제약 분야 적용을 통해 글로벌 양자 기술 허브로 발전을 추진함. ✓ https://opengovasia.com/싱가포르-stronger-quantum-talent-and-research-infrastructure/?c=global

[싱가포르] 온라인 서비스 장애	▸ **통신사와 은행, 메신저 등 온라인 서비스에서 일시적 장애가 증가하고 있음(3월 23일)** ✓ 싱가포르에서 3월 23일 인터넷 기반 서비스 장애가 발생했으며 Singtel에서 가장 큰 영향이 나타남. ✓ Downdetector 기준 신고가 약 9,800건까지 급증했으나 약 15분 내 빠르게 감소함. ✓ StarHub, M1, Discord, WhatsApp 등 다양한 서비스에서도 동시 장애가 보고됨. ✓ Singtel은 원인을 국제 트래픽 최적화 문제로 설명하며 로컬 네트워크는 정상 상태였다고 밝힘. ✓ 전문가들은 라우팅 오류 등 글로벌 네트워크 문제로 발생한 일시적 장애로 분석하며 빠르게 복구된 사례로 평가함. ✓ https://www.straitstimes.com/싱가포르/telcos-banks-chat-apps-among-net-based-services-to-experience-temporary-spike-in-disruptions
[싱가포르] (3월 23일) 랜섬웨어 공격	▸ **Trio-Tech International의 싱가포르 자회사가 랜섬웨어 공격으로 데이터가 유출돼 온라인에 공개됐음(3월 23일)** ✓ Trio-Tech International 싱가포르 자회사가 랜섬웨어 공격으로 파일 암호화와 데이터 유출 피해를 입었음. ✓ 3월 11일 발생한 공격 이후 시스템 오프라인 전환과 외부 전문가 및 수사기관 협력이 진행됨. ✓ 초기에는 영향이 제한적이라 평가됐으나 데이터 공개 이후 중대한 보안 사고로 재평가됨. ✓ 공격은 Gunra 랜섬웨어 조직의 이중 협박 Double Extortion 방식으로 분석됨. ✓ 이번 사례는 공급망 기업도 주요 표적이 되며 초기 과소평가 이후 리스크가 확대되는 패턴을 보여줌. ✓ https://cryptobriefing.com/trio-tech-싱가포르-ransomware-attack/

[싱가포르] (3월 24일) 주요 네트워크 회복력 강화	▸ **싱가포르가 주요 네트워크 회복력 강화를 위한 스마트 대책을 추진하고 있음(3월 24일)** ✓ 싱가포르가 통신 장애 상황에서도 신속한 대응으로 높은 디지털 회복력을 보여줌. ✓ IMDA(Infocomm Media Development Authority)가 즉각 조사와 점검에 착수해 서비스 안정성 확보에 나섬. ✓ 장애는 결제·배달 등 서비스에 영향을 줬으나 사이버 공격이 아닌 기술적 문제로 확인됨. ✓ 당국은 기계적 결함과 소프트웨어 문제를 원인으로 분석하며 인프라 복잡성을 반영한 사례로 평가함. ✓ 정부와 Singtel 협력을 통해 복구와 개선 조치를 추진하며 국가 차원의 회복력 강화 방향을 보여줌. ✓ https://opengovasia.com/싱가포르-smart-measures-strengthen-critical-network-resilience/?c=global
[싱가포르] (3월 30일) 중소기업 사이버보안	▸ **싱가포르 중소기업들이 AI 도입을 확대하며 사이버보안 강화 필요성이 커지고 있음(3월 30일)** ✓ 싱가포르가 2026년 예산에서 AI(Artificial Intelligence)를 국가 경제 성장의 핵심 축으로 강조하며 기업 지원을 확대함. ✓ IMDA(Infocomm Media Development Authority)에 따르면 전체 사이버 공격의 약 40퍼센트가 SME(Small and Medium-sized Enterprises)를 겨냥함. ✓ 기업들은 높은 보안 자신감과 달리 실제 사고 경험이 많아 준비 수준과 현실 간 격차가 존재함. ✓ AI 확산으로 디지털 환경이 복잡해지며 기존 보안 체계만으로는 대응이 어려워지고 있음. ✓ 전문가들은 클라우드 기반 보안과 가시성 확보를 통해 AI 시대에 맞는 보안 기반 구축이 필수적이라고 강조함. ✓ https://sbr.com.sg/economy/commentary/싱가포르s-smes-are-embracing-ai-cybersecurity-must-keep

[말레이시아] AI 거버넌스	▸ **말레이시아가 혁신과 지식재산 보호를 위한 AI 거버넌스를 추진하고 있음(3월 3일)** ✓ 말레이시아가 AI(Artificial Intelligence) 기술의 법적·윤리적 위험 관리를 위해 Artificial Intelligence Governance Bill 제정을 추진함. ✓ 해당 법안은 AI 학습과 배포 전 과정의 위험 관리와 개발자·이용자 지침 제공을 목표로 함. ✓ 저작권 데이터 활용 문제와 지식재산권 침해 가능성이 주요 쟁점으로 논의됨. ✓ 법안은 Copyright Act 1987을 보완하며 전 생애주기 위험 평가와 투명성, 감사 체계 구축을 요구함. ✓ AI 거버넌스는 국가결제게이트웨이(National Payment Gateway/GPN) 등 기존 디지털 인프라와 조화를 이루며 공공 신뢰 확보를 목표로 함. ✓ https://opengovasia.com/말레이시아-ai-governance-to-protect-innovation-intellectual-property/?c=global
[말레이시아] 데이터유출 단속 국제공조	▸ **말레이시아가 LeakBase(데이터유출 정보공유 온라인 커뮤니티) 단속을 위한 국제 공조에 참여했음(3월 6일)** ✓ 말레이시아 MACC(말레이시아n Anti-Corruption Commission)가 LeakBase 포럼 해체를 위한 국제 공조 수사에 참여함. ✓ 해당 작전은 Europol 주도로 FBI(Federal Bureau of Investigation), United States Department of Justice 등 14개국이 협력함. ✓ 말레이시아에서는 쿠알라룸푸르 웹 호스팅 업체 대상 압수수색과 디지털 증거 확보가 진행됨. ✓ LeakBase는 2021년부터 운영된 불법 데이터 거래 플랫폼으로 계정 정보와 금융 데이터가 유통됨. ✓ 이번 수사는 국제 협력을 통한 사이버 범죄 대응과 디지털·금융 시스템 보호 의지를 보여줌. ✓ https://www.scoop.my/news/283590/말레이시아-joins-global-crackdown-on-leakbase-cybercrime-forum/

[말레이시아] 기술 및 디지털 인프라	▸ **말레이시아의 기술 및 디지털 인프라가 기록적 투자 유치를 이끌고 있음 (3월 9일)** ✓ 말레이시아가 2025년 총 4,267억 링깃 투자 유치로 역대 최고치를 기록함. ✓ 전년 대비 약 11퍼센트 증가했으며 8,390개 프로젝트를 통해 약 24만 개 일자리 창출이 예상됨. ✓ 국내 투자 51.5퍼센트, 외국인 투자 증가로 투자 구조가 균형 있게 확대됨. ✓ 서비스 부문이 최대 비중을 차지하며 ICT(Information and Communication Technology)와 AI(Artificial Intelligence) 기반 투자가 성장 견인함. ✓ 데이터센터와 첨단 제조 투자 확대를 통해 기술 중심 경제 전환과 경쟁력 강화가 추진됨. ✓ https://opengovasia.com/말레이시아-technology-and-digital-infrastructure-fuel-record-investment/?c=global
[말레이시아] 하이브리드 전쟁 위협 대응	▸ **말레이시아는 하이브리드 전쟁 위협 대응을 위해 사이버 및 기술 방어 역량 강화를 요구받고 있음(3월 10일)** ✓ 말레이시아가 하이브리드 전쟁 대응을 위해 국방 역량과 신기술 도입 확대 필요성이 제기됨. ✓ MIDAS(말레이시아n Institute of Defence and Security) 연구원은 현대 전쟁이 사이버 공격과 정보전 등 디지털 요소와 결합된 형태라고 설명함. ✓ 물리적 공격과 함께 공항, 금융 네트워크 등 디지털 인프라 마비 가능성이 강조됨. ✓ 말레이시아는 무역과 인프라 의존도가 높아 사이버 공격 시 경제적 영향이 클 것으로 분석됨. ✓ NDIP(National Defence Industry Policy) 기반으로 사이버 방어, 산업 협력, 인재 양성 강화 필요성이 제시됨. ✓ https://www.nst.com.my/amp/news/nation/2026/03/1393237/말레이시아-must-boost-cyber-tech-defences-against-hybrid-warfare-threats

[말레이시아] 기업들의 주요 사이버 컴플라이언스	▸ **말레이시아 기업들의 주요 사이버 컴플라이언스 실수와 예방 방안이 제시됨(3월 11일)** ✓ 말레이시아에서 Cyber Security Act 2024 시행으로 기업의 사이버보안 준수 요구가 크게 강화됨. ✓ NCII(National Critical Information Infrastructure) 지정 조직은 위험 평가, 보안 감사, 사고 보고 의무를 수행해야 함. ✓ 전문가들은 보안을 일회성 대응이 아닌 지속적인 관리 체계로 운영해야 한다고 강조함. ✓ 경영진과 이사회 차원의 거버넌스와 사고 대응 플레이북 및 모의 훈련 필요성이 제시됨. ✓ ISO/IEC 27001과 별개로 법적 격차 분석과 제3자 리스크 관리, 감사 기록 강화가 중요함. ✓ https://www.mexc.com/news/895024
[말레이시아] 증권사의 사이버 사고	▸ **Bursa 말레이시아는 증권사 수준에서 발생한 사이버 사고가 통제됐다고 밝혔음(3월 12일)** ✓ Bursa 말레이시아에서 일부 증권사 사이버보안 사건이 발생했으나 시장 운영에는 영향이 없었음. ✓ 해당 증권사들은 문제 시스템을 즉시 격리하고 사고 대응 절차를 가동함. ✓ 조사 결과 사건은 개별 증권사에 국한됐으며 거래소 인프라에는 영향이 없었음. ✓ 무단 거래나 금융 손실 증거는 발견되지 않았으며 신속한 대응으로 확산이 차단됨. ✓ 거래소는 전사적 보안 점검과 함께 2026년 4분기까지 IT 보안 기준 강화를 추진함. ✓ https://www.thestar.com.my/business/business-news/2026/03/12/bursa-말레이시아-broker-level-cyber-incidents-contained
[말레이시아] 주식시스템 사이버보안 점검	▸ **Malacca Securities가 시스템 점검을 위해 말레이시아 주식 거래를 중단했음(3월 24일)** ✓ Malacca Securities Sdn Bhd가 예방적 사이버보안 점검을 위해 3월 24일부터 말레이시아 주식 거래를 일시 중단함. ✓ 조치는 제3자 OMS(Order Management System) 공급업체 관련 보안 점검으로 규제 지침에 따라 시행됨. ✓ 모바일 앱, 웹, 딜러 채널 주문이 중단되고 기존 GTC (Good 'til Canceled) , GTC (Good 'til Canceled) 주문도 취소됨. ✓ 미국·홍콩 거래는 정상 유지되며 고객 자산은 안전하게 보호되고 있음. ✓ 이번 사례는 제3자 벤더 리스크와 금융권 사이버보안 관리 중요성을 보여줌. ✓ https://theedge말레이시아.com/node/797232

[말레이시아] 경제 회복력 강화를 위한 핵심 기술 역량	▸ **말레이시아가 경제 회복력 강화를 위해 핵심 기술 역량을 강화하고 있음(3월 30일)** ✓ 말레이시아가 반도체, AI(Artificial Intelligence), 희토류, 사이버보안 등 핵심 기술 분야 투자 확대를 추진함. ✓ 해당 전략은 MKN(Majlis Keselamatan Negara) 중심으로 국가 회복력과 글로벌 공급망 역할 강화를 목표로 함. ✓ 반도체 생산·패키징 강점을 바탕으로 전자·자동차 산업 공급망에서 핵심 국가로 자리잡고 있음. ✓ 희토류 개발과 AI 활용 확대를 통해 미래 산업 기반과 보안 역량을 동시에 강화함. ✓ 사이버보안 기술과 디지털 인프라 보호를 결합해 지속 가능한 성장과 기술 자율성 확보를 추진함. ✓ https://opengovasia.com/말레이시아-strengthens-critical-tech-to-boost-economic-resilience/?c=global
[필리핀] 아동 온라인 안전	▸ **Philippines에서 아동 온라인 안전을 위해 디지털 부모 교육 중요성이 강조되고 있음(3월 10일)** ✓ 필리핀 중앙 비사야스에서 OSAEC(Online Sexual Abuse and Exploitation of Children) 증가로 부모 역할 강화 필요성이 제기됨. ✓ 사회복지개발부 DSWD(Department of Social Welfare and Development)는 디지털 부모 역할의 중요성을 강조함. ✓ 부모는 자녀의 플랫폼 사용을 이해하고 올바른 온라인 행동을 직접 보여줘야 함. ✓ 2025년 최소 50명 아동이 구조됐으며 아동 스스로 위험 콘텐츠를 제작하는 사례도 증가함. ✓ 정부는 상담·교육·지역 협력을 통해 예방을 강화하며 열린 소통의 중요성을 강조함. ✓ https://opengovasia.com/the-philippines-digital-parenting-key-to-childrens-online-safety/?c=global
[필리핀] 디지털 아세안 구축	▸ **필리핀이 디지털 경제 프레임워크 협정을 통해 회복력 있고 포용적인 디지털 아세안 구축을 추진하고 있음(3월 12일)** ✓ 아세안이 마닐라에서 DEFA(Digital Economy Framework Agreement) 협상을 진행하며 디지털 경제 협력을 추진함. ✓ 필리핀 의장국 주도로 ASEAN Secretariat과 회원국, 전문가들이 협정 초안을 검토함. ✓ DEFA는 디지털 무역 확대와 국경 간 경제 통합, 상호운용 가능한 디지털 환경 구축을 목표로 함. ✓ 디지털 결제, 전자 문서, 온라인 사기 대응을 통해 SME 참여 확대가 기대됨. ✓ 법률 검토 후 아세안 정상회의에서 최종 서명을 목표로 하며 지역 디지털 경제 성장 기반을 강화함. ✓ https://opengovasia.com/the-philippines-defa-to-build-a-resilient-and-inclusive-digital-asean/?c=global

[필리핀] 국가 디지털 신분증	▸ **필리핀이 더 빠르고 안전한 서비스 제공을 위해 국가 디지털 신분증 도입을 추진하고 있음(3월 25일)** ✓ Philippine Statistics Authority가 PhilSys(Philippine Identification System) 등록 확대를 통해 디지털 서비스 접근성 강화를 추진함. ✓ 국가 신분증은 단일 신원 인증 수단으로 행정 절차 간소화와 공공·민간 서비스 이용을 지원함. ✓ 지방정부와 협력한 방문 등록 및 PhilSys on Wheels로 취약계층 접근성이 확대됨. ✓ 신분증 사칭 피싱 등 보안 위협 증가에 따라 사용자 주의 필요성이 강조됨. ✓ 안전한 인증과 활용을 통해 포용적이고 효율적인 디지털 사회 구축이 목표로 제시됨. ✓ https://opengovasia.com/the-philippines-national-id-for-smarter-faster-safer-services/?c=global
	▶ **시사점 및 국내 보안 기업 진출 포인트** ✓ (인도네시아) 동남아 데이터센터 허브로 주목받는 경향. 3월 중 아동의 온라인 안전을 위해 소셜미디어 이용제한이 시행. 사이버보안 기본법 제정논의가 지속되고 있음 => 아동 보호조치 관련 기술 ✓ (싱가포르) 사이버보안 강국답게 AI 가속화 정책, 양자컴퓨팅 대응 연구 등이 지속 추진되고 있음 => AI, 양자암호 관련 기술 ✓ (말레이시아) ICT 및 AI 등에 투자규모가 커지고 있으며, 기술역량이 경제에 기여하는 바가 클 것으로 보고 지속 지원중임 => AI 관련 기술

정보보호 해외진출 전략거점(중남미) 3월 주요동향

2026. 3. 31.(화), 한국인터넷진흥원 AI보안산업본부 AI보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[멕시코] 정부 기관 대상 Claude Code 악용 사이버 공격 발생	▸ **생성형 AI 도구를 활용한 지능형 공격 시연 및 공공 부문 보안 취약성 노출(3월 1일)** ✓ 해커들이 앤스로픽(Anthropic)의 코딩 보조 AI 도구인 'Claude Code'를 악용하여 멕시코 정부 기관의 시스템 취약점을 찾아내고 익스플로잇을 작성하는 데 성공함 ✓ 공격자들은 AI의 가드레일을 우회하는 정교한 프롬프트 엔지니어링 기술을 사용하여 보안 필터를 통과하고 단시간 내에 고도화된 악성코드를 생성함 ✓ 이번 공격은 단순한 데이터 탈취를 넘어 AI가 사이버 무기화되어 실제 정부 인프라 타격에 사용될 수 있음을 보여준 사례로 평가됨 ✓ 멕시코 국세청(SAT)과 선거관리위원회(INE) 등 주요 기관의 레거시 시스템이 주요 타겟이 되었으며, AI 자동화 도구로 인해 공격의 속도와 규모가 비약적으로 증가함 ✓ 보안 전문가들은 AI 기반 공격이 인간의 대응 속도를 상회하므로, 방어 측면에서도 AI 기반의 실시간 위협 탐지 및 대응 시스템 도입이 필수적임을 강조함 ✓ 정부 부문의 노후화된 소프트웨어 업데이트와 패치 관리 소홀이 공격자들에게 최적의 침투 경로를 제공하고 있음이 재확인됨 ✓ 공격자들은 버그 바운티 테스터로 위장하거나 합법적인 개발 도구를 활용하는 사회 공학적 기법을 병행하여 탐지를 회피함 ✓ 이번 사건은 국가 디지털 자산 보호를 위해 생성형 AI 위협에 특화된 새로운 보안 거버넌스와 방어 아키텍처 수립이 시급함을 시사함 ✓ 멕시코 내 보안 커뮤니티는 AI 기술의 이면인 사이버 범죄 활용 가능성에 대해 경고하며 민관 합동 대응 체계 구축을 촉구함 ✓ 공공 인프라의 탄력성 확보를 위해 단순 솔루션 도입을 넘어 지속적인 취약점 점검과 AI 위협 시뮬레이션 훈련이 요구됨 ✓ https://www.securityweek.com/hackers-weaponize-claude-code-in-mexican-government-cyberattack/
[콜롬비아] 영국과 사이버 보안 전략적 대화 및 협력 강화	▸ **글로벌 보안 선진국과의 파트너십을 통한 기술 전수 및 정책 공조 확대(3월 2일)** ✓ 콜롬비아 외교부와 영국 정부는 사이버보안 분야의 전략적 파트너십을 강화하고 기술 협력 및 정보 공유를 위한 고위급 대화를 진행함 ✓ 양국은 지능형 사이버 범죄 대응, 국가 핵심 인프라 보호, 사이버 공간의 책임 있는 국가 행동 규범 수립 등에 대해 논의함 ✓ 영국은 자국의 우수한 보안 모델과 침해 사고 대응(CSIRT) 운영 노하우를 콜롬비아에 공유하고 전문가 교류 프로그램을 지원하기로 함 ✓ 콜롬비아 내 보안 인력 양성을 위해 영국의 전문 교육 커리큘럼을 도입하고 공동 연구 프로젝트를 추진하는 방안이 검토됨 ✓ 디지털 경제의 신뢰 구축을 위해 국제적인 보안 표준과 인증 체계를 콜롬비아 시장에 안착시키기 위한 협력이 강화됨

이 슈	주 요 내 용 및 시 사 점
	✓ 양국은 랜섬웨어 등 국경을 넘는 사이버 범죄를 척결하기 위해 법 집행 기관 간의 실시간 공조 체계를 공고히 하기로 합의함 ✓ 이번 협력은 콜롬비아가 유럽의 선진 보안 기술과 정책을 수용하여 자국의 보안 수준을 국제적 기준으로 격상시키는 기폭제가 될 것으로 기대됨 ✓ 사이버보안을 중심으로 한 디지털 외교를 강화하여 양국의 경제 협력을 뒷받침할 안전한 디지털 환경을 조성하는 데 주력함 ✓ 영국의 민간 보안 기업들이 콜롬비아 시장에 진출할 수 있는 토대를 마련하고 현지 기업들과의 기술 제휴를 독려함 ✓ 콜롬비아는 이번 전략적 대화를 통해 중남미 지역 내 사이버보안 협력의 허브 역할을 수행하겠다는 비전을 제시함 ✓ https://www.cancilleria.gov.co/newsroom/news/colombia-reino-unido-fortalecen-dialogo-estrategico-materia-ciberseguridad
[칠레] 사이버보안 프레임워크 법 시행 및 효율적 이행 과제	▸ **국가 사이버보안 역량 강화를 위한 법적 토대 마련 및 민관 협력 가이드라인 제시(3월 3일)** ✓ 칠레 정부가 제정한 '사이버보안 프레임워크 법(Ley Marco de Ciberseguridad)'의 본격적인 시행을 앞두고 구체적인 이행 전략과 도전 과제가 논의됨 ✓ 이 법안은 국가사이버보안국(ANCI) 설립을 포함하며, 국가 핵심 인프라 운영 기관에 엄격한 보안 표준 준수 의무를 부여함 ✓ 기업들은 법적 규제 준수를 단순한 비용이 아닌 경쟁력 확보와 비즈니스 신뢰를 위한 전략적 투지로 인식해야 함 ✓ 전문가들은 법안의 성공적인 안착을 위해 실질적인 기술 가이드라인 제공과 중소기업을 위한 보안 지원 대책이 병행되어야 한다고 조언함 ✓ 침해사고 발생 시 즉각적인 보고 체계를 확립하고 부문별 컴퓨터 침해사고 대응반(CSIRT)과의 협력을 강화하는 것이 핵심임 ✓ 칠레 내 보안 전문가 부족 현상을 해결하기 위해 학계 및 산업계가 연계한 실무 중심의 보안 교육 커리큘럼 개발이 촉구됨 ✓ 디지털 주권 확보를 위해 국제 표준(ISO/IEC 27001 등)을 현지 환경에 맞게 내재화하고 인증 체계를 정비하는 노력이 지속됨 ✓ 규제 위반 시 부과되는 강력한 제재 조치는 기업들이 선제적인 보안 투자를 집행하게 만드는 촉매제 역할을 할 것으로 기대됨 ✓ 사이버보안 거버넌스를 체계화하여 국가 차원의 위기 관리 능력을 높이고 글로벌 보안 인덱스 순위를 상향시키려는 목표를 가짐 ✓ 이번 법안은 칠레 디지털 경제의 안전한 성장을 뒷받침하는 근간이자 중남미 지역의 보안 입법 모델이 될 것으로 평가됨 ✓ https://www.trendtic.cl/2026/03/ley-marco-de-ciberseguridad-de-chile-y-la-necesidad-de-internalizar-los-desafios-directrices-y-su-eficiente-cumplimiento/
[멕시코] 정부 기관 대상 사이버 공격, AI 기반 위협의 현실성 증명	▸ **AI 기술이 접목된 공격 도구의 위험성 경고 및 공공 보안 아키텍처 재설계 촉구(3월 6일)** ✓ 최근 발생한 멕시코 정부 기관 대상 사이버 공격에서 공격자들이 AI를 활용해 취약점 분석과 스피어 피싱 메일 작성을 자동화한 것으로 드러남 ✓ AI 기반 공격 도구는 기존 보안 솔루션의 탐지 패턴을 학습하여 이를 우회하는 변종 악성코드를 실시간으로 생성하는 능력을 보여줌

이 슈	주 요 내 용 및 시 사 점
	✓ 보안 전문가들은 AI가 공격의 진입 장벽을 낮추고 대규모 공격을 소수의 인원으로도 가능하게 만들고 있다고 경고함 ✓ 멕시코 공공 부문의 레거시 인프라는 이러한 지능형 공격에 무방비 상태이며, 전면적인 보안 시스템 현대화가 시급한 시점임 ✓ 정부는 AI 위협에 대응하기 위해 자체적으로 AI 기반의 위협 탐지 및 자동 차단 시스템 도입을 서두르고 있음 ✓ 이번 사례는 AI 기술이 양날의 검임을 보여주며, 국가 보안 정책에 AI 리스크 관리와 윤리적 활용 가이드라인이 포함되어야 함을 시사함 ✓ 공격자들은 생성형 AI를 사용하여 고도로 정교해진 사회 공학적 공격을 수행하며 공무원들의 계정 정보를 성공적으로 탈취함 ✓ 보안 업계는 'AI에는 AI로 대응(AI vs AI)'하는 전략이 유일한 해결책임을 강조하며 지능형 보안 플랫폼 도입을 권고함 ✓ 국가 핵심 정보 자산 보호를 위해 데이터 중심의 보안(Data-centric security)과 영구적 모니터링 체계 구축이 필수적임 ✓ 멕시코는 이번 공격을 계기로 공공 인프라 보호를 위한 차세대 보안 아키텍처 로드맵을 전면 재검토할 예정임 ✓ https://www.darkreading.com/application-security/cyberattack-mexico-government-ai-threat
[파라과이] 폴란드와 안보 및 사이버보안 협력 강화 합의	▸ **국방·안보 분야의 국제 공조를 통한 기술 교류 및 보안 역량 강화 추진 (3월 10일)** ✓ 파라과이 정부는 폴란드 대표단과 회담을 갖고 국방 및 사이버 보안 분야의 전략적 협력을 강화하기 위한 양해각서(MOU)를 체결함 ✓ 양국은 사이버 범죄, 테러리즘, 하이브리드 위협에 공동 대응하기 위해 기술 정보를 공유하고 전문가 파견 및 교육 프로그램을 운영하기로 함 ✓ 특히 폴란드의 우수한 사이버 방어 기술과 국가 보안 관제 노하우를 파라과이의 국가 시스템에 이식하기 위한 프로젝트가 시작됨 ✓ 파라과이 국방부는 폴란드와의 협력을 통해 군사 네트워크의 보안 수준을 높이고 사이버 전담 부서의 대응 능력을 고도화할 계획임 ✓ 이번 협력은 동유럽과 중남미 국가 간의 보안 협력이라는 점에서도 의의가 있으며, 글로벌 위협에 대한 범지역적 대응 전선을 구축함 ✓ 양국은 디지털포렌식, 암호 기술, 국가 핵심 인프라 보호 전략 등에 대한 공동 워크숍과 훈련을 정례화하기로 함 ✓ 폴란드 보안 기업들의 파라과이 시장 진출을 지원하고 현지 파트너사와의 기술 제휴를 독려하는 비즈니스 포럼이 개최됨 ✓ 파라과이는 이번 협력을 통해 유럽의 선진 보안 표준을 수용하고 자국 내 보안 인프라를 현대화하는 기회로 활용하려 함 ✓ 지정학적 긴장이 고조되는 상황에서 양국은 사이버 공간의 평화와 안정을 유지하기 위한 국제 규범 수립에도 목소리를 같이하기로 함 ✓ 이번 파트너십은 파라과이가 글로벌 보안 네트워크의 일원으로 참여하여 국가 안보의 외연을 확장하는 계기가 될 것으로 평가됨 ✓ https://www.masencarnacion.com/articulo/paraguay-y-polonia-fortalecen-cooperacion-en-seguridad-y-ciberseguridad
[우루과이] 현지 해커 조직, 최초의 100% 자체 개발 랜섬웨어 유포	▸ **지역 맞춤형 공격 도구의 출현 및 변종 악성코드에 따른 보안 위협의 국지화(3월 10일)**

이 슈	주 요 내 용 및 시 사 점
	✓ 우루과이의 사이버 범죄 조직이 기존 해외 소스 코드를 빌리지 않고 100% 자체 기술로 개발한 최초의 국산 랜섬웨어를 제작·유포하여 충격을 줌 ✓ 이 랜섬웨어는 우루과이 내 공공 기관과 기업들의 시스템 환경에 최적화되어 개발되었으며, 현지 언어와 사회적 맥락을 이용한 정교한 피싱 수법을 사용함 ✓ 보안 전문가들은 자체 개발된 악성코드가 기존 글로벌 백신 솔루션의 탐지 패턴에 등록되어 있지 않아 식별하기 매우 어렵고 위험하다고 경고함 ✓ 공격자들은 암호화된 데이터를 인질로 금전을 요구할 뿐만 아니라, 우루과이 정부의 보안 정책을 조롱하는 메시지를 남기는 등 대담한 행보를 보임 ✓ 이번 사건은 우루과이 내 사이버 범죄 기술 수준이 독자적인 공격 도구를 제작할 만큼 고도화되었음을 보여주는 상징적인 사례임 ✓ 우루과이 사이버 센터(CERT.uy)는 해당 랜섬웨어의 샘플을 확보하여 분석 중이며, 주요 기관들에 긴급 방어 지침을 하달함 ✓ 전문가들은 지역 맞춤형 공격(Localized Attack)에 대응하기 위해 현지 위협 인텔리전스를 실시간으로 수집하고 대응할 수 있는 특화된 보안 체계가 필요하다고 제언함 ✓ 이번 사고로 인해 우루과이 내 소프트웨어 공급망 보안과 내부 네트워크 모니터링의 중요성이 재조명됨 ✓ 정부는 사이버 범죄 수사 역량을 총동원하여 해당 조직을 추적하고 있으며, 악성코드 개발 및 유포에 대한 처벌 수위를 상향할 방침임 ✓ 시민들에게는 출처가 불분명한 현지 메일이나 링크에 대해 각별한 주의를 당부하고 최신 보안 업데이트를 즉시 적용할 것을 권고함 ✓ https://www.elobservador.com.uy/ciencia-y-tecnologia/ciberatacantes-crean-el-primer-ransomware-100-uruguayo-n6036845
[온두라스] 미국 지원 기반 사이버보안 및 통신 인프라 강화 추진	▶ **양국 간 기술 협력을 통한 5G 보안 및 국가 사이버 방어 역량 고도화 (3월 11일)** ✓ 온두라스 정부는 미국 대표단과 만나 사이버 보안 강화 및 디지털 인프라 현대화를 위한 협력 방안을 심도 있게 논의함 ✓ 미국은 온두라스의 국가 보안 수준을 높이기 위해 기술적 컨설팅과 보안 장비 지원, 전문 인력 교육 프로그램을 제공하기로 함 ✓ 양국은 5G 통신망 구축 과정에서 발생할 수 있는 보안 위협을 최소화하기 위해 신뢰할 수 있는 공급망 확보의 중요성에 공감함 ✓ 온두라스 내 국가 침해 사고 대응 센터(CERT)의 역량을 강화하고 실시간 위협 정보를 공유하는 핫라인 구축이 추진됨 ✓ 이번 협력은 온두라스가 디지털 경제로 전환하는 과정에서 지정학적 안보 리스크를 관리하고 국가 인프라의 투명성을 높이려는 목적을 가짐 ✓ 사이버 범죄 소탕을 위한 법 집행 기관 간의 공조를 강화하고 디지털포렌식 기술 전수를 확대하기로 함 ✓ 정부 부처의 노후화된 IT 시스템을 클라우드 기반의 안전한 환경으로 이전하기 위한 로드맵 수립에 미국의 지원이 투입됨 ✓ 온두라스는 미국의 기술 지원을 통해 국제적인 보안 표준을 도입하고 중남미 내 보안 허브로서의 입지를 다지고자 함 ✓ 민간 부문의 보안 인식 제고를 위해 양국 상공회의소가 주도하는 보안 컨퍼런스 및 비즈니스 매칭 행사를 정례화할 계획임 ✓ 이번 파트너십은 온두라스의 디지털 주권을 강화하고 외국인 투자를 유치할 수 있는 안전한 비즈니스 환경을 조성하는 데 기여할 것으로 평가됨

이 슈	주 요 내 용 및 시 사 점
	✓ https://www.elheraldo.hn/honduras/estados-unidos-honduras-abordan-temas-tecnologia-ciberseguridad-HE29692234
[페루] 기업 10곳 중 4곳, 심각한 사이버 보안 사고 경험 보고	▶ **침해 사고의 보편화와 대응 역량 부족에 따른 산업 전반의 보안 위기감 고조(3월 11일)** ✓ 최근 조사에 따르면 페루 기업의 약 38%가 지난 한 해 동안 운영에 차질을 빚을 정도의 심각한 사이버 공격을 받은 것으로 나타남 ✓ 주요 공격 유형으로는 랜섬웨어가 가장 많았으며, 피싱을 통한 계정 탈취와 내부자에 의한 정보 유출 사고도 높은 비중을 차지함 ✓ 조사 대상 기업의 상당수가 공격 발생 후 이를 인지하기까지 평균 수주 이상의 시간이 소요되어 피해 규모를 키운 것으로 분석됨 ✓ 페루 내 보안 전문가들은 기업들이 침해 사고 대응 계획(IRP)을 실효성 있게 갖추고 정기적인 훈련을 실시해야 한다고 촉구함 ✓ 특히 보안 예산이 부족한 중소기업들이 사이버 범죄 조직의 손쉬운 타겟이 되고 있어 범국가적 지원 대책 마련이 시급함 ✓ 해커들은 페루 기업들의 취약한 원격 근무 환경과 패치되지 않은 VPN 서버를 주요 침투 경로로 악용하고 있음 ✓ 이번 보고서는 페루 산업계 전반에 보안 경종을 울렸으며, 기업들이 보안 솔루션 도입과 인력 확보를 서두르는 계기가 됨 ✓ 정부는 사이버 범죄 피해 신고를 독려하고 피해 기업들을 위한 기술 지원 및 복구 컨설팅을 제공할 계획임 ✓ 보안 업계는 실시간 가시성을 확보할 수 있는 통합 보안 플랫폼 도입이 사각지대를 제거하고 사고를 조기에 발견하는 핵심임을 강조함 ✓ 페루 기업들은 이제 '언제 공격받을 것인가'에 대비하여 탐지 및 대응(Detection & Response) 역량을 강화하는 방향으로 투자를 전환하고 있음 ✓ https://www.infobae.com/peru/2026/03/12/ciberataques-en-peru-casi-4-de-cada-10-empresas-reportan-incidentes-graves-de-seguridad/
[과테말라] 개인정보 및 뱅킹 데이터 노린 사이버 공격 집중 발생	▶ **사이버 공격의 절반 이상이 금전적 이득을 목적으로 한 금융 정보 탈취에 집중(3월 12일)** ✓ 과테말라에서 발생하는 사이버 공격의 약 50%가 개인 신원 정보 및 은행 계좌 정보를 탈취하여 직접적인 금전적 이득을 취하려는 시도로 분석됨 ✓ 공격자들은 피싱 사이트, 악성 광고(Malvertising), 가짜 모바일 뱅킹 앱 등 다양한 수법을 동원하여 사용자의 인증 정보를 수집함 ✓ 특히 사회 공학적 기법을 통해 은행 상담원을 사칭하거나 공공 기관 안내를 위장하여 피해자를 속이는 사례가 빈번하게 보고됨 ✓ 과테말라 금융권은 고객 보호를 위해 생체 인증 및 기기 식별 기술을 도입하고 있으나, 사용자들의 보안 의식 부족이 여전히 취약점으로 작용함 ✓ 다크웹에서는 과테말라 시민들의 유출된 신용카드 정보와 개인정보 데이터베이스가 활발하게 거래되고 있는 것으로 파악됨 ✓ 보안 업체들은 기업들이 고객 데이터를 암호화하여 저장하고 내부 직원의 데이터 접근 권한을 엄격히 제한할 것을 권고함 ✓ 랜섬웨어 공격이 금융 기관의 백오피스 시스템을 겨냥하면서 운영 중단 리스크와 데이터 복구 비용 문제가 심각하게 대두됨 ✓ 정부는 사이버 범죄 수사팀의 역량을 강화하고 통신사들과 협력하여 악성 URL 차단 및 스팸 메시지 필터링 시스템을 고도화하고 있음

이 슈	주 요 내 용 및 시 사 점
	✓ 이번 통계는 과테말라 내 보안 투자가 금융 보안 및 신원 관리(IAM) 분야에 최우선적으로 집중되어야 함을 보여줌 ✓ 대국민 보안 수칙 교육을 강화하고 의심스러운 링크 클릭 방지 등 예방 중심의 보안 문화 정착이 시급한 과제임 ✓ https://www.prensalibre.com/economia/la-mitad-de-los-ciberataques-en-guatemala-van-por-la-informacion-personal-y-bancaria/
[코스타리카] 전력공사(ICE) 시스템 침투 및 내부 이메일 유출 사고 발생	▸ **국가 핵심 에너지·통신 인프라 대상 사이버 스파이 활동 포착 및 데이터 탈취 확인(3월 12일)** ✓ 코스타리카 전력공사(ICE)의 내부 네트워크에 해커들이 침투하여 수천 건의 내부 이메일과 민감 정보를 탈취한 대규모 보안 사고가 발생함 ✓ 조사 결과 공격자들은 수개월 전부터 시스템에 잠입하여 지속적인 정보 유출 활동을 벌였으며, 주요 경영진과 기술진의 계정이 탈취된 것으로 확인됨 ✓ 이번 사고는 국가 핵심 인프라인 전력 및 통신망의 제어 시스템까지 위협받을 수 있었던 중대한 사안으로 파악되어 국가 위기관리 센터가 가동됨 ✓ 탈취된 데이터에는 인프라 운영 계획, 고객 정보, 협력사 계약 내용 등 민감한 비즈니스 데이터가 포함되어 있어 2차 피해가 우려되는 상황임 ✓ ICE 측은 침입 경로를 확인하고 관련 서버를 긴급 격리하였으나, 이미 상당 부분의 데이터가 외부로 전송된 상태임을 인정함 ✓ 보안 전문가들은 이번 공격이 고도로 숙련된 그룹에 의해 수행되었으며, 지능형 지속 위협(APT) 기법이 동원된 것으로 분석함 ✓ 내부 시스템의 취약한 인증 절차와 사각지대에 놓였던 레거시 서버가 초기 침투 경로로 의심받고 있음 ✓ 이번 유출 사고로 인해 공공 서비스에 대한 시민들의 불안감이 커지고 있으며, 정부의 보안 관리 책임에 대한 거센 비판이 일고 있음 ✓ ICE는 전면적인 시스템 현대화와 제로 트러스트 기반 인증 체계 도입을 선언하고 외부 전문 보안 업체와 함께 정밀 포렌식을 진행 중임 ✓ 국가 차원의 사이버 방어망을 재점검하고 핵심 인프라 운영 기관들에 대한 보안 표준 준수 실태 조사가 전격 실시됨 ✓ https://www.infobae.com/costa-rica/2026/03/12/hackers-lograron-infiltrarse-en-sistemas-del-instituto-costarricense-de-electricidad-y-robar-informacion-de-correos-internos/
[코스타리카] 정부, ICE 사이버 스파이 공격 배후로 중국 연계 조직 지목	▸ **지정학적 리스크와 결합된 사이버 안보 위협 공식화 및 외교적 대응 시사(3월 12일)** ✓ 코스타리카 정부는 최근 발생한 전력공사(ICE) 해킹 사건의 배후에 중국과 연계된 사이버 스파이 조직이 있다는 분석 결과를 공식 발표함 ✓ 정부 관계자는 공격 기법과 사용된 악성코드의 특성을 분석한 결과, 특정 국가의 지원을 받는 해킹 그룹의 소행일 가능성이 매우 높다고 밝힘 ✓ 이번 발표는 코스타리카가 국가 인프라에 대한 외부 세력의 개입을 공식적으로 규탄한 이례적인 사례로, 국제 사회의 관심을 모으고 있음 ✓ 공격자들은 코스타리카의 전략적 자산과 기술 정보를 수집하기 위해 정교한 스파이웨어와 맞춤형 공격 도구를 사용한 것으로 드러남 ✓ 중국 측은 해당 의혹을 즉각 부인하였으나, 코스타리카 정부는 기술적 증거를 바탕으로 국제 사회와 공조하여 추가 조사를 진행하겠다는 입장임

이 슈	주 요 내 용 및 시 사 점
	✓ 이번 사건으로 인해 코스타리카 내 5G 통신망 구축 등 주요 인프라 사업에서 특정 국가 장비 배제 논란이 재점화될 것으로 보임 ✓ 보안 전문가들은 국가 배후 공격의 타겟이 된 만큼, 방어 체계를 군사적 수준의 사이버 보안 아키텍처로 격상시켜야 한다고 제언함 ✓ 우방국들과의 위협 인텔리전스 공유를 통해 유사한 패턴의 공격 시도를 사전에 차단하기 위한 협력을 강화하고 있음 ✓ 내부 조력자 존재 여부 및 사회 공학적 기법 활용 가능성에 대해서도 심도 있는 수사가 진행 중임 ✓ 코스타리카는 이번 사고를 계기로 국가 디지털 주권 수호를 위한 강력한 법적, 기술적 방어선 구축에 박차를 가할 예정임 ✓ https://observador.cr/gobierno-de-costa-rica-denuncia-ciberespionaje-chino-en-el-ice/
[브라질] Rust 기반 VENON 악성코드, 33개 주요 은행 타겟 공격	▸ **고도화된 프로그래밍 언어를 활용한 신종 악성코드 출현 및 금융권 보안 위협 증대(3월 12일)** ✓ 브라질 내 33개 금융 기관을 노린 'VENON'이라는 이름의 Rust 기반 신종 악성코드가 발견되어 금융권에 비상이 걸림 ✓ 이 악성코드는 탐지를 회피하기 위해 Rust 언어로 제작되었으며, 사용자 기기에 침투하여 정교한 오버레이(Overlay) 창을 띄워 금융 인증 정보를 탈취함 ✓ 공격자들은 합법적인 소프트웨어 업데이트로 위장하거나 피싱 메일을 통해 악성코드를 배포하며 피해자의 뱅킹 앱 실행을 실시간으로 감시함 ✓ 탈취된 정보에는 사용자 ID, 비밀번호뿐만 아니라 2단계 인증(2FA) 코드까지 포함되어 실질적인 금전적 피해로 직결됨 ✓ 보안 전문가들은 기존 시그니처 기반 탐지 솔루션이 Rust 기반 악성코드를 식별하는 데 한계가 있음을 지적하고 행동 기반 탐지 강화를 권고함 ✓ 브라질 금융권은 PIX 실시간 결제 시스템의 보안성을 높이기 위해 다요소 인증(MFA)과 기기 지문 인식 기술 도입을 서두르고 있음 ✓ 이번 공격은 사이버 범죄 조직이 더욱 효율적이고 강력한 프로그래밍 언어를 사용하여 공격 도구를 진화시키고 있음을 보여줌 ✓ 금융 기관들은 실시간 위협 모니터링 체계를 가동하고 고객들에게 신종 피싱 수법에 대한 주의보를 발령함 ✓ 엔드포인트 보안(EDR) 강화와 함께 비정상 거래 탐지 시스템(FDS)의 고도화가 금융 보안의 핵심 과제로 부상함 ✓ 국경을 넘나드는 사이버 범죄 조직에 대응하기 위해 국제 수사 기관과의 공조 및 보안 인텔리전스 공유가 시급한 시점임 ✓ https://thehackernews.com/2026/03/rust-based-venon-malware-targets-33.html
[도미니카공화국] UNAPEC 대학, 사이버 보안 석사 과정 신설 발표	▸ **고도화된 위협에 대응할 전문 인력 양성을 위한 고등 교육 커리큘럼 도입(3월 16일)** ✓ 도미니카공화국의 UNAPEC 대학교는 국가 사이버보안 수준을 한 단계 끌어올릴 핵심 인재 육성을 위해 새로운 사이버 보안 석사 학위 과정을 개설함 ✓ 해당 과정은 최신 사이버 위협 분석, 디지털포렌식, 정보보호 거버넌스, 클라우드 보안 등 실무 중심의 고도화된 커리큘럼으로 구성됨

이 슈	주 요 내 용 및 시 사 점
	✓ 국가 전체적으로 보안 전문가 수요가 급증함에 따라 현직 IT 전문가 및 정부 관계자들을 대상으로 전문성을 심화할 수 있는 기회를 제공함 ✓ UNAPEC 대학은 글로벌 보안 기업들과 파트너십을 맺고 실무 환경과 유사한 보안 실습 랩(Lab)을 구축하여 학생들의 대응 역량을 키울 계획임 ✓ 이번 석사 과정 신설은 도미니카공화국 내 보안 교육의 질을 국제적 수준으로 높이고 자생적인 보안 생태계를 조성하는 데 기여할 것으로 보임 ✓ 졸업생들은 공공 및 민간 부문의 정보보호 최고책임자(CISO)로 활동하며 국가 디지털 자산 보호의 핵심 역할을 수행하게 됨 ✓ 대학 측은 이론 교육뿐만 아니라 윤리적 해킹(Ethical Hacking) 및 사고 대응 모의 훈련을 강화하여 실질적인 문제 해결 능력을 강조함 ✓ 사이버 보안 교육의 대중화를 위해 온라인 강의 시스템을 도입하고 직장인들을 위한 유연한 학사 운영을 실시함 ✓ 이번 조치는 국가 사이버 안보 역량 강화를 위해 교육계가 적극적으로 동참한 모범 사례로 평가받으며 타 교육 기관으로의 확산이 기대됨 ✓ 정부는 해당 과정을 수료한 인재들이 공공 기관 보안 부서에 우선 채용될 수 있도록 지원 방안을 검토 중임 ✓ https://diariodigitalrd.com/2026/03/16/unapec-presenta-maestria-clave-para-la-ciberseguridad-del-pais.html/
[도미니카공화국] Indotel 청장, 디지털 교육 및 사이버 보안 우선순위 강조	▸ **미래 인재 양성 및 범국민적 보안 인식 제고를 통한 디지털 경쟁력 확보(3월 19일)** ✓ 도미니카공화국 통신청(Indotel) 청장은 국가 발전을 위해 디지털 기술 교육과 사이버 보안 역량 강화가 정부의 최우선 과제가 되어야 한다고 역설함 ✓ 디지털 대전환 시대에 국민들이 안전하게 기술을 누리기 위해서는 기본적인 보안 수칙 준수와 위협 식별 능력을 갖추는 것이 필수적임 ✓ Indotel은 청년층과 취약 계층을 대상으로 한 대대적인 디지털 리터러시 교육 프로그램을 런칭하고 보안 교육 콘텐츠를 무상으로 배포함 ✓ 특히 사이버 보안 분야의 만성적인 인력 부족 문제를 해결하기 위해 산학 협력 기반의 전문 자격증 과정 신설을 적극 지원함 ✓ 기업 경영진들에게는 보안을 비용이 아닌 비즈니스 연속성을 위한 필수 투자로 인식하고 보안 문화 조성에 앞장설 것을 당부함 ✓ 정부는 초고속 인터넷망 보급 확대와 병행하여 해당 인프라의 보안성을 높이기 위한 기술적 방어막 구축에 예산을 집중 투입함 ✓ 온라인 사기 및 피싱 범죄로부터 시민들을 보호하기 위해 유관 기관과의 합동 단속과 피해 예방 홍보를 강화하고 있음 ✓ 디지털 교육은 단순히 기기 사용법을 가르치는 것을 넘어 개인정보 보호와 윤리적 기술 활용을 포함하는 포괄적인 방향으로 추진됨 ✓ 이번 발표는 도미니카공화국이 중남미 디지털 경제의 주역으로 성장하기 위해 인적 자본의 보안 역량을 강화하겠다는 강력한 의지를 반영함 ✓ Indotel은 향후 글로벌 기술 기업들과 협력하여 최신 보안 교육 인프라를 구축하고 지역 내 보안 교육 허브로 거듭나겠다는 비전을 제시함 ✓ https://www.presidencia.gob.do/noticias/presidente-del-indotel-exhorta-priorizar-formacion-digital-y-ciberseguridad

이 슈	주 요 내 용 및 시 사 점
[코스타리카] 국가 사이버 보안 전략(2023-2027) 분석 및 보완론 대두	▸ **전략적 안일함(Strategic Naiveté) 경계 및 실질적 방어 실행력 확보 요구(3월 19일)** ✓ 코스타리카의 '국가 사이버 보안 전략 2023-2027'에 대한 심층 분석 결과, 선언적 목표에 비해 구체적인 실행 계획과 예산 뒷받침이 부족하다는 비판이 제기됨 ✓ 전문가들은 국가 보안 정책이 기술적 현실을 충분히 반영하지 못하는 '전략적 순진함'에서 벗어나 실질적인 위협 기반 대응 체계로 전환되어야 한다고 강조함 ✓ 특히 공공 부문의 전문 인력 부족과 노후화된 인프라 문제가 전략 이행의 가장 큰 걸림돌로 지목되며 긴급 자금 투입의 필요성이 역설됨 ✓ 보고서는 랜섬웨어 공격자들의 진화 속도를 정부의 대응 속도가 따라잡지 못하고 있음을 지적하며 신속한 의사결정 구조 마련을 촉구함 ✓ 민간 부문의 보안 자산을 국가 방어 체계에 유기적으로 통합하기 위한 인센티브 제도와 법적 보호 장치 마련이 시급함 ✓ 글로벌 보안 기업들과의 파트너십을 통해 최신 위협 탐지 기술을 도입하고 국산 보안 솔루션의 고도화를 지원하는 투자가 병행되어야 함 ✓ 국가 핵심 정보 시스템에 대한 전면적인 보안 감사를 실시하고 취약점 노출 지수를 정기적으로 공개하여 책임성을 강화해야 함 ✓ 사이버보안 교육을 정규 교육 과정에 포함시켜 미래 인재를 양성하는 중장기적인 관점의 인적 자원 투자가 제안됨 ✓ 이번 분석은 코스타리카가 디지털 주권을 실질적으로 확보하기 위해 문서상의 전략을 넘어 강력한 실행력을 갖춘 보안 거버넌스로 진화해야 함을 시사함 ✓ 정부는 제기된 비판을 수용하여 전략의 이행 로드맵을 수정 보완하고 범부처 협력 체계를 재정비할 계획임 ✓ https://www.larepublica.net/noticia/costa-rica-entre-la-ciberseguridad-y-la-ingenuidad-estrategica-analisis-ala-estrategia-nacional-de-ciberseguridad-de-costa-rica-2023-2027
[중남미] 볼리비아·콜롬비아·에콰도르·페루 SMB 대상 보안 강화 촉구	▸ **안데스 지역 중소기업(SMB)의 사이버 회복 탄력성 확보를 위한 가이드라인 보급(3월 21일)** ✓ 볼리비아, 콜롬비아, 에콰도르, 페루 4개국 보안 전문가들은 역내 중소기업(SMB)들이 급증하는 사이버 공격의 주요 타겟이 되고 있음을 경고하고 보안 강화를 권고함 ✓ 중소기업들은 대기업에 비해 보안 예산과 인력이 부족하여 랜섬웨어 및 피싱 공격에 매우 취약하며, 이는 전체 공급망 리스크로 번질 수 있음 ✓ 전문가들은 SMB가 도입하기 적합한 클라우드 기반 구독형 보안 서비스(SaaS)와 저비용·고효율 보안 도구 활용을 적극 추천함 ✓ 직원들을 대상으로 한 기본적인 보안 교육이 공격의 90% 이상을 예방할 수 있음을 강조하며 정기적인 교육 실시를 촉구함 ✓ 각국 정부는 SMB의 디지털 전환을 지원하는 동시에 보안 진단 및 컨설팅을 제공하는 지원 프로그램을 확대할 계획임 ✓ 다요소 인증(MFA) 도입, 운영체제 및 소프트웨어의 적시 패치, 중요 데이터의 오프라인 백업이 SMB를 위한 3대 핵심 보안 수칙으로 제시됨 ✓ 역내 협력을 통해 SMB 전용 위협 정보 공유 플랫폼을 구축하고 사고 발생 시 공동 대응할 수 있는 네트워크를 마련함

이 슈	주 요 내 용 및 시 사 점
	✓ 보안은 기술적 문제가 아니라 비즈니스 생존의 문제임을 인식하고 경영진이 직접 보안 전략을 챙겨야 한다는 점이 강조됨 ✓ 안데스 공동체(CAN) 차원의 통합 보안 표준을 마련하여 국경을 넘는 이커머스 거래의 안전성을 확보하려는 노력이 지속됨 ✓ 이번 권고는 지역 내 경제의 허리 역할을 하는 SMB들을 보호함으로써 국가 전체의 디지털 경제 안정성을 유지하려는 목적을 가짐 ✓ https://lavozdetarija.com/2026/03/21/convocan-a-pymes-de-bolivia-colombia-ecuador-y-peru-a-fortalecer-su-ciberseguridad-y-resiliencia-digital/
[도미니카공화국] Indotel-DNI, 국가 사이버 보안 강화를 위한 업무협약 체결	▸ **통신 규제 기관과 정보 기관의 협력을 통한 실시간 위협 대응 체계 구축(3월 22일)** ✓ 도미니카 통신청(Indotel)과 국가정보국(DNI)은 국가 사이버 공간 보호와 정보 인프라 안전성 확보를 위한 전략적 업무협약(MOU)을 체결함 ✓ 양 기관은 사이버 공격 징후를 조기에 발견하고 공동 대응하기 위해 실시간 위협 정보 공유 메커니즘을 구축하기로 합의함 ✓ 특히 국가 핵심 정보 통신망을 노린 지능형 위협에 대비하여 민관 합동 보안 관제 시스템의 효율성을 높이는 데 주력함 ✓ Indotel은 통신 사업자들의 보안 표준 준수 여부를 감독하고, DNI는 국가 안보 차원의 사이버 스파이 및 범죄 조직 추적 활동을 강화함 ✓ 이번 협약에는 사이버 보안 분야의 전문 인력 양성과 공무원 대상의 보안 인식 교육 프로그램 공동 운영이 포함됨 ✓ 디지털 금융 및 이커머스 확산에 따른 개인정보 유출 사고 예방을 위해 관련 법규 정비와 기술적 가이드라인 보급에 협력함 ✓ 국가 위기 상황 발생 시 신속한 의사결정을 돕는 비상 연락 체계를 정비하고 부문별 CSIRT 간의 유기적인 협조를 독려함 ✓ 정부 관계자는 이번 협약이 국가 보안 거버넌스를 체계화하고 부처 간 장벽을 허물어 대응 역량을 극대화하는 계기가 될 것이라고 밝힘 ✓ 도미니카공화국은 이를 통해 사이버 공격에 대한 국가적 회복 탄력성을 높이고 안전한 디지털 경제 생태계를 조성하고자 함 ✓ 향후 국제 보안 기관과의 네트워크를 확장하여 글로벌 위협에 선제적으로 대응할 수 있는 글로벌 협력 체계를 강화할 계획임 ✓ https://acento.com.do/actualidad/indotel-y-dni-firman-acuerdo-para-fortalecer-la-ciberseguridad-en-republica-dominicana-9645572.html
[과테말라] 법적 프레임워크 부재 속 고도화되는 사이버 공격에 직면	▸ **사이버 범죄 처벌 및 보안 표준 확립을 위한 입법 지연과 이에 따른 안보 공백 우려(3월 22일)** ✓ 과테말라는 최근 지능형 사이버 공격이 빈번하게 발생하고 있으나, 이를 규제하고 처벌할 수 있는 국가 차원의 사이버 보안법이 없어 대응에 한계를 겪고 있음 ✓ 해커 조직들은 과테말라의 법적 공백을 악용하여 정부 시스템과 금융망을 공격 표적으로 삼고 있으며, 공격의 정교함이 갈수록 높아지는 추세임 ✓ 보안 전문가들은 과테말라가 국제 사이버 범죄 협약(부다페스트 협약 등)에 가입하고 국내법을 정비하는 것이 시급하다고 강력히 주장함 ✓ 현재는 사이버 사고 발생 시 명확한 보고 의무나 대응 프로토콜이 없어 초기 진압과 피해 복구에 많은 시간이 소요됨

이 슈	주 요 내 용 및 시 사 점
	✓ 공공 기관의 디지털 자산을 보호하기 위한 예산 할당이 법적 근거 부족으로 인해 매년 순위에서 밀리는 실정임 ✓ 기업들은 자체적으로 글로벌 보안 표준을 도입하려 노력 중이나, 국가 차원의 가이드라인 부재로 인해 보안 수준의 양극화가 심화되고 있음 ✓ 정부 내 보안 컨트롤타워 기능을 수행할 전담 기구의 설립이 법안 통과 지연으로 인해 표류하고 있는 상황임 ✓ 이번 위기는 과테말라가 디지털 전환 정책을 추진하기에 앞서 안전한 법적·제도적 인프라를 먼저 구축해야 함을 시사함 ✓ 시민들의 개인정보 보호를 위한 데이터 보호법 제정도 시급하며, 이를 위반하는 행위에 대한 엄격한 처벌 조항 마련이 요구됨 ✓ 국회 내 보안 관련 법안 처리를 위한 초당적 협력이 촉구되며, 글로벌 보안 파트너들과의 협력을 통한 입법 지원이 논의 중임 ✓ https://www.prensalibre.com/guatemala/justicia/guatemala-enfrenta-ciberataques-cada-vez-mas-sofisticados-sin-un-marco-legal-solido/
[파나마] 신뢰·AI·디지털 사기, 보안 컨퍼런스 주요 화두로 부상	▸ **Ciberilatam 행사를 통한 중남미 보안 트렌드 공유 및 민관 협력 강화(3월 23일)** ✓ 파나마에서 열린 사이버 보안 행사 'Ciberilatam'에서 디지털 신뢰 구축, AI의 보안 활용, 그리고 진화하는 디지털 사기 대응 방안이 집중 논의됨 ✓ 참가자들은 AI 기술이 공격자들에게는 정교한 공격 도구가 되고 방어자들에게는 강력한 탐지 수단이 되는 '기술적 군비 경쟁' 상황임을 진단함 ✓ 특히 딥페이크(Deepfake)를 활용한 피싱과 자동화된 봇넷 공격 등 디지털 사기 수법이 고도화됨에 따라 이에 대한 공동 대응이 촉구됨 ✓ 디지털 환경에서의 '신뢰'가 비즈니스 성패를 결정짓는 핵심 요소로 부각되며, 제로 트러스트 보안 모델의 도입 필요성이 역설됨 ✓ 파나마 금융권은 AI 기반의 이상 거래 탐지 시스템(FDS) 구축 사례를 공유하고 고객 데이터 보호를 위한 협력 방안을 모색함 ✓ 전문가들은 보안이 단순한 도구 도입을 넘어 조직 전체의 전략과 문화로 내재화되어야 한다고 조언함 ✓ 정부 관계자는 사이버 보안 강화를 위한 최신 법안 제정 추진 현황을 설명하고 민간 부문의 적극적인 참여와 의견 개진을 요청함 ✓ 중소기업들을 위한 맞춤형 보안 가이드라인과 클라우드 보안 서비스 활용법에 대한 실무 세션이 진행되어 큰 호응을 얻음 ✓ 이번 행사는 파나마가 중남미 내 보안 지식 공유와 기술 교류의 중심지로 성장하고 있음을 보여주는 계기가 됨 ✓ 국경 없는 사이버 위협에 대응하기 위해 인근 국가들과의 실시간 인텔리전스 공유 및 합동 수사 체계 구축이 강조됨 ✓ https://www.segurilatam.com/ciberilatam/ciberseguridad-ciberilatam/la-confianza-la-ia-y-el-fraude-digital-protagonistas-del-ultimo-evento-de-ciberseguridad-en-panama_20260323.html
[칠레] 디지털 회복 탄력성 및 AI 중심의 보안 아젠다 확산	▸ **2026년 칠레 은행 및 정부 보안 컨퍼런스를 통한 국가 보안 전략 논의(3월 23일)** ✓ 칠레에서 개최된 'Cybersecurity Bank & Government 2026' 행사에서 디지털 회복 탄력성과 인공지능이 국가 보안의 핵심 키워드로 부각됨

이 슈	주 요 내 용 및 시 사 점
	✓ 금융권과 정부 기관 관계자들은 지능형 위협에 대응하기 위해 AI를 방어 체계의 중심에 두는 전략적 전환의 필요성에 공감함 ✓ 단순한 공격 차단을 넘어 사고 발생 시 비즈니스 연속성을 보장할 수 있는 사이버 탄력성(Cyber Resilience) 확보가 최우선 과제로 제시됨 ✓ 칠레의 새로운 사이버보안 프레임워크 법(Ley Marco) 시행에 따른 공공 및 민간 부문의 규제 준수 가이드라인이 상세히 논의됨 ✓ 랜섬웨어와 피싱 등 고도화된 공격으로부터 국가 핵심 인프라를 보호하기 위한 제로 트러스트(Zero Trust) 모델 도입이 강조됨 ✓ 전문가들은 보안이 단순 IT 부서의 업무가 아닌 이사회 수준에서 다뤄져야 할 전략적 리스크 관리 요소임을 역설함 ✓ 디지털 금융 전환이 가속화됨에 따라 데이터 보호와 프라이버시 확보가 고객 신뢰 구축의 핵심 자산으로 인식됨 ✓ 민간과 공공 부문의 실시간 위협 정보 공유 체계 구축을 통해 범국가적인 대응 역량을 상향 표준화하려는 노력이 지속됨 ✓ 최신 보안 기술 트렌드인 머신러닝 기반 이상 징후 탐지 및 자동화된 사고 대응(SOAR) 솔루션에 대한 관심이 집중됨 ✓ 이번 행사는 칠레가 라틴아메리카 내 보안 선도 국가로 도약하기 위한 기술적, 제도적 로드맵을 확립하는 계기가 됨 ✓ https://www.trendtic.cl/2026/03/resiliencia-digital-e-inteligencia-artificial-marcan-la-agenda-del-cybersecurity-bank-government-chile-2026/
[브라질] 정부 디지털 전환에 따른 사이버 위협 및 회복력 강화	▸ **국가적 차원의 디지털 서비스 확대와 이에 따른 보안 리스크 관리 전략 수립(3월 25일)** ✓ 브라질 정부의 광범위한 디지털 전환 정책으로 인해 공공 서비스의 접점이 늘어남과 동시에 사이버 공격 표적도 확대되는 양상을 보임 ✓ 정부 시스템 보호를 위해 위험 기반 접근 방식(Risk-based approach)을 도입하고 국가적 차원의 사이버보안 탄력성 로드맵을 가동함 ✓ 공공 부문의 데이터 유출 사고 예방을 위해 데이터 암호화 및 엄격한 접근 제어 시스템 구축에 대규모 예산이 투입될 예정임 ✓ 브라질 사이버보안 전문가들은 정부 기관 간의 파편화된 보안 체계를 통합하고 중앙 집중식 보안 관제 센터의 기능을 강화해야 한다고 제언함 ✓ 디지털 격차 해소와 동시에 보안 인식을 제고하기 위한 범국가적 캠페인 및 전문 보안 인력 양성 프로그램이 병행됨 ✓ 클라우드 네이티브 환경으로의 전환 과정에서 발생하는 설정 오류 및 권한 관리 취약점이 주요 보안 도전 과제로 지목됨 ✓ 국가 핵심 인프라 보호를 위해 국제 보안 표준을 준수하고 정기적인 보안 감사를 의무화하는 법적 장치 마련이 추진 중임 ✓ 지능형 지속 위협(APT)에 대응하기 위해 위협 인텔리전스 공유 플랫폼을 고도화하고 민관 협력을 극대화하는 방안이 논의됨 ✓ 이번 전환 과정은 브라질이 안전하고 신뢰할 수 있는 디지털 정부를 구현하기 위한 필수적인 진통이자 도약의 기회로 평가됨 ✓ 시민의 개인정보 보호를 최우선 가치로 설정하고 설계 단계부터 보안(Security by Design)을 적용하는 문화 정착에 주력함 ✓ https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2026.1779065/full

이 슈	주 요 내 용 및 시 사 점
[도미니카공화국] Thales-MIDAS 컨소시엄 주도로 전자여권 현대화 추진	▸ **차세대 생체 인식 기술 기반의 보안 문서 발급 체계 구축 및 국가 신뢰도 제고(3월 25일)** ✓ 도미니카공화국 정부는 글로벌 보안 기업 탈레스(Thales)와 MIDAS 컨소시엄을 사업자로 선정하고 전자여권 도입 및 현대화 프로젝트를 본격화함 ✓ 이번 프로젝트는 기존 종이 여권을 최첨단 생체 인식 칩이 내장된 전자여권으로 전면 교체하여 위변조를 근본적으로 차단하는 데 목적이 있음 ✓ 전자여권에는 사용자의 지문, 안면 정보 등 고정밀 생체 데이터가 암호화되어 저장되며, 국제민간항공기구(ICAO)의 보안 표준을 엄격히 준수함 ✓ 탈레스의 고성능 운영 체제와 보안 솔루션을 적용하여 여권 발급 프로세스의 효율성을 높이고 국경 통제 시스템과의 실시간 연동을 강화함 ✓ 도미니카 시민들은 전자여권 도입으로 해외 여행 시 입국 심사 시간을 단축하고 비자 면제 혜택 확대 등 이동의 편의성이 증대될 것으로 기대됨 ✓ 정부는 여권 발급 센터의 인프라를 현대화하고 데이터 보호를 위해 강력한 보안 관리 체계를 구축할 계획임 ✓ 이번 현대화 사업은 국가 디지털 아이덴티티 전략의 일환으로, 안전한 신원 인증 기반을 통해 디지털 행정 서비스의 신뢰도를 높이려는 목적을 가짐 ✓ 글로벌 보안 기술을 현지에 도입함으로써 도미니카공화국의 디지털 보안 위상을 중남미 내 선도적인 수준으로 격상시킬 것으로 평가됨 ✓ 프로젝트 진행 과정에서 현지 인력에 대한 기술 전수 및 운영 교육이 포함되어 국내 기술 자생력 확보에도 기여할 예정임 ✓ 차세대 전자여권은 도미니카공화국의 국가 브랜드 이미지를 개선하고 국제 시장에서의 신뢰를 얻는 핵심 자산이 될 것으로 보임 ✓ https://www.businesswire.com/news/home/20260324368065/en/Dominican-Republic-Drives-Modernization-of-Electronic-Passports-Under-the-Leadership-of-the-Thales---MIDAS-Consortium
[페루] 비즈니스 연속성을 위한 사이버 보안의 전략적 가치 부각	▸ **디지털 전환의 안정성 확보를 위한 보안 거버넌스 및 회복 탄력성 강화(3월 25일)** ✓ 페루의 디지털 경제 성장이 가속화됨에 따라 기업의 영속성을 담보하기 위한 사이버 보안의 역할이 그 어느 때보다 중요해짐 ✓ 사이버 공격은 이제 기술적 장애를 넘어 기업의 재무 상태와 대외 신뢰도에 직접적인 영향을 미치는 전략적 리스크로 진화함 ✓ 기업들은 공격을 완벽히 막는 것이 불가능하다는 전제 하에 사고 피해를 최소화하고 신속히 복구하는 '탄력성' 중심의 보안 아키텍처를 지향함 ✓ 페루 내 주요 산업 섹터(금융, 에너지, 광업)를 중심으로 제로 트러스트 모델과 AI 기반 보안 자동화 도구 도입이 확산되고 있음 ✓ 전문가들은 보안 투자가 디지털 혁신을 가속화하고 고객에게 안전한 서비스를 제공하는 비즈니스 활성화 장치(Enabler)임을 역설함 ✓ 정부는 국가 차원의 사이버 보안 탄력성을 높이기 위해 공공 인프라와 민간 기업 간의 위협 정보 공유 체계를 고도화하고 있음 ✓ 경영진의 보안 인식을 높이기 위해 이사회 수준의 보안 리스크 보고 체계를 수립하고 보안 성과 지표(KPI)를 도입하는 기업이 늘고 있음 ✓ 고객 프라이버시 보호를 위한 국제 표준 인증 획득이 글로벌 시장 진출을 위한 페루 기업들의 필수 과제로 부상함

이 슈	주 요 내 용 및 시 사 점
	✓ 이번 트렌드는 페루 보안 문화가 사후 대응에서 선제적 예방 및 거버넌스 강화 단계로 성숙해지고 있음을 보여줌 ✓ 보안 파트너사와의 협력을 통해 24/7 실시간 모니터링 시스템을 구축하고 지능화되는 위협에 능동적으로 대처하려는 노력이 지속됨 ✓ https://www.revistaeconomia.com/ciberataques-en-aumento-por-que-la-continuidad-de-las-empresas-en-peru-depende-de-su-ciberseguridad/
[중남미] 라틴아메리카 5개국 대상 악성코드 위협 순위 발표	▸ **브라질·멕시코·콜롬비아 등 주요국의 위협 노출도 분석 및 대응 촉구 (3월 26일)** ✓ 중남미 지역의 최신 사이버 위협 보고서에 따르면 브라질, 멕시코, 콜롬비아, 페루, 에콰도르 5개국이 악성코드 공격의 주요 타겟으로 조사됨 ✓ 특히 브라질은 라틴아메리카에서 가장 높은 공격 빈도를 기록했으며, 금융 정보를 노린 뱅킹 트로이목마와 랜섬웨어가 기승을 부리고 있음 ✓ 멕시코는 공공 기관과 제조업을 타겟으로 한 공급망 공격 및 데이터 탈취 시도가 빈번하게 발생하며 위협 순위 2위를 기록함 ✓ 공격자들은 지능형 지속 위협(APT) 기법을 사용하여 타겟 시스템에 장기 체류하며 기밀 정보를 빼내는 수법을 선호하는 것으로 나타남 ✓ 조사 결과 유출된 계정 정보를 이용한 신원 도용 공격이 급증하고 있으며, 이는 다중 클라우드 환경의 설정 오류에서 기인하는 경우가 많음 ✓ 전문가들은 중남미 국가들이 사이버 범죄의 '테스트베드'가 되고 있다고 경고하며, 국가 차원의 강력한 방어선 구축이 시급하다고 역설함 ✓ 악성코드의 배포 경로로 소셜 엔지니어링과 취약한 소프트웨어 공급망이 지목되어 이에 대한 집중적인 모니터링이 요구됨 ✓ 지역 내 국가 간 위협 인텔리전스 공유가 부족하여 동일한 공격 패턴에 반복적으로 피해를 입는 사례가 다수 확인됨 ✓ 기업들은 엔드포인트 보안과 더불어 네트워크 내부의 측면 이동(Lateral Movement)을 감지할 수 있는 보안 솔루션 도입을 서둘러야 함 ✓ 이번 랭킹은 중남미 국가들이 사이버 안보를 국가적 우선순위로 설정하고 국제적인 보안 공조를 강화해야 함을 시사함 ✓ https://www.infobae.com/tecno/2026/03/26/ranking-de-ciberataques-los-5-paises-de-latinoamerica-bajo-la-mira-del-malware/
[파나마] Ericsson, 5G와 사이버보안 통합의 중요성 강조	▸ **차세대 통신 인프라 구축의 핵심 전제 조건으로서의 보안 및 디지털 전환 전략(3월 27일)** ✓ 글로벌 통신 장비 기업 에릭슨(Ericsson)은 파나마의 디지털 전환을 위해 5G 도입 시 사이버 보안이 설계 단계부터 통합되어야 한다고 제언함 ✓ 5G 네트워크는 수많은 IoT 기기와 핵심 인프라를 연결하므로, 보안 취약점이 발생할 경우 국가 전체에 치명적인 영향을 미칠 수 있음 ✓ 에릭슨은 파나마 정부와 통신 사업자들에게 신뢰할 수 있는 공급망 관리와 엔드투엔드(End-to-End) 암호화 기술 도입을 권고함 ✓ 5G 기반의 스마트 시티, 자율 주행, 원격 의료 등 혁신 서비스를 안전하게 제공하기 위한 보안 가이드라인 수립이 논의됨 ✓ 전문가들은 5G의 개방형 아키텍처가 새로운 보안 도전 과제를 제시하며, 이를 해결하기 위한 지능형 네트워크 모니터링이 필수적임을 강조함 ✓ 파나마는 지역 내 물류 및 금융 허브로서 5G와 보안의 결합을 통해 글로벌 경쟁력을 높이려는 전략적 목표를 가지고 있음

이 슈	주 요 내 용 및 시 사 점
	✓ 이번 발표는 5G 기술 도입이 단순한 속도 향상을 넘어 국가 안보 수준을 강화하는 계기가 되어야 함을 시사함 ✓ 에릭슨은 자사의 글로벌 보안 경험을 바탕으로 파나마 현지 인력 교육과 보안 관제 기술 이전을 지원할 준비가 되어 있다고 밝힘 ✓ 5G 시대의 사이버 보안은 기술적 방어를 넘어 경제적 번영과 사회적 신뢰를 유지하는 근간이 될 것으로 평가됨 ✓ 파나마 정부는 에릭슨의 제안을 수렴하여 5G 라이선스 조건에 보안 표준 준수 항목을 강화하는 방안을 검토 중임 ✓ https://revistasumma.com/ericsson-destaca-en-panama-la-importancia-de-integrar-ciberseguridad-y-5g-para-impulsar-una-transformacion-digital/
[페루] 사이버 공격, 기업 비즈니스 연속성 심각하게 위협	▸ **운영 중단 및 데이터 유출에 따른 경제적 손실 증대와 보안 투자 시급성 강조(3월 27일)** ✓ 페루 내 기업들이 랜섬웨어 및 디도스(DDoS) 공격으로 인한 시스템 중단 사태를 겪으며 비즈니스 연속성에 심각한 타격을 입고 있음 ✓ 보안 사고 발생 시 페루 기업들이 겪는 평균 복구 비용과 생산성 손실이 매년 증가하고 있으며, 이는 기업 생존을 위협하는 수준에 도달함 ✓ 전문가들은 단순한 방화벽 도입을 넘어 사고 발생 시 신속하게 복구할 수 있는 '비즈니스 연속성 계획(BCP)' 수립이 필수적이라고 조언함 ✓ 페루 기업들의 약 40%가 최근 1년 내 심각한 보안 침해 사고를 경험했으나, 이에 대한 적절한 대응 지침을 갖춘 곳은 소수에 불과함 ✓ 특히 고객 데이터 유출은 브랜드 평판 실추와 법적 소송으로 이어져 기업 경영에 치명적인 영향을 미칠 수 있음이 경고됨 ✓ 정부는 기업들의 보안 수준을 높이기 위해 사이버 보안 가이드라인을 보급하고 사고 보고 체계를 정비하고 있음 ✓ 중소기업들은 클라우드 보안 서비스를 활용하여 저비용으로 고도화된 방어 체계를 갖추려는 시도를 늘려가는 추세임 ✓ 보안 전문가들은 정기적인 취약점 점검과 임직원 보안 교육이 공격 피해를 최소화하는 가장 효과적인 방법임을 강조함 ✓ 페루 내 보안 시장은 비즈니스 회복 탄력성을 돕는 백업 및 복구 솔루션, 실시간 위협 관제 서비스를 중심으로 수요가 확대되고 있음 ✓ 이번 상황은 페루 기업들이 보안을 '선택'이 아닌 '필수' 경영 자산으로 재정의하고 공격적인 투자를 집행해야 함을 시사함 ✓ https://www.mercadonegro.pe/medios/digital/tecnologia/ciberseguridad-peru/
[도미니카공화국] 사이버 보안·보건·주권 간 연계를 통한 전략적 신뢰 구축	▸ **보건 의료 데이터 보호를 국가 주권 및 신뢰의 핵심 자산으로 정의 (3월 27일)** ✓ 도미니카공화국은 보건 의료 시스템의 디지털화에 맞춰 사이버 보안을 국가 주권과 시민의 안전을 담보하는 핵심 전략 자산으로 선언함 ✓ 병원 및 의료 기관을 노린 랜섬웨어 공격이 환자의 생명과 직결될 수 있다는 인식 하에 의료 데이터 보호를 위한 특화된 보안 가이드라인을 수립함 ✓ 의료 정보 시스템의 가동 중단을 막기 위한 고가용성 인프라 구축과 데이터 불변 백업 솔루션 도입에 예산을 우선 배정함

이 슈	주 요 내 용 및 시 사 점
	✓ 전문가들은 '신뢰'가 디지털 의료 서비스의 성공을 결정짓는 핵심 지표이며, 이를 위해 강력한 프라이버시 보호 기술이 뒷받침되어야 한다고 역설함 ✓ 정부는 보건 의료 부문의 사이버 보안 수준을 점검하기 위한 전수 조사를 실시하고 보안 사고 발생 시 즉각 대응 프로토콜을 정립함 ✓ 환자의 민감한 의료 기록이 다크웹 등 외부로 유출되는 것을 차단하기 위해 데이터 암호화 및 접근 이력 추적 시스템을 강화함 ✓ 사이버 보안은 이제 단순 기술 영역을 넘어 국가 안보와 국민 복지를 연결하는 통합적인 거버넌스 차원에서 다뤄지고 있음 ✓ 국제적인 보건 보안 표준을 도입하여 도미니카 의료 시스템의 글로벌 신뢰도를 높이고 외국인 환자 유치 등 의료 관광 활성화를 도모함 ✓ 민간 의료 기관들과의 협력을 통해 보안 투자 비용 부담을 줄일 수 있는 공동 보안 관제 서비스(MSSP) 모델 보급을 추진함 ✓ 이번 전략은 도미니카공화국이 안전한 디지털 보건 국가로 성장하기 위한 중요한 이정표가 될 것으로 평가됨 ✓ https://listindiario.com/la-vida/20260327/ciberseguridad-salud-soberania-confianza-activo-estrategico-rd_899379.html
[콜롬비아] 지정학적 긴장 고조에 따른 사이버 공격 경계령 발령	▸ **미국–이란 간 갈등 등 글로벌 정세 변화가 콜롬비아 내 사이버 위협에 미치는 영향 분석(3월 28일)** ✓ 미국과 이란 사이의 지정학적 긴장이 고조됨에 따라 콜롬비아 내 주요 공공기관과 기업을 향한 사이버 공격 시도가 급증하며 경계 태세가 강화됨 ✓ 국가 배후 해킹 그룹들이 우방국인 콜롬비아의 에너지, 금융, 정부 네트워크를 타겟으로 정보 탈취 및 시스템 마비 공격을 시도할 가능성이 제기됨 ✓ 콜롬비아 사이버 사령부와 경찰청 사이버 센터는 실시간 모니터링 수위를 높이고 주요 기반 시설 운영사들에게 보안 패치 업데이트를 긴급 권고함 ✓ 전문가들은 지정학적 갈등이 사이버 공간에서의 대리전으로 번질 수 있으며, 콜롬비아가 그 전초 기지가 될 위험이 있다고 경고함 ✓ 공격자들은 분산 서비스 거부(DDoS) 공격이나 파괴형 와이퍼(Wiper) 악성코드를 사용하여 사회적 혼란을 야기할 수 있음이 지적됨 ✓ 민간 기업들은 공급망 보안을 점검하고 외부 위협 인텔리전스 서비스를 활용하여 잠재적 공격 징후를 조기에 포착하려는 노력을 기울임 ✓ 정부는 국제 사회와의 공조를 통해 위협 정보를 실시간으로 공유하고 공동 방어 전선을 구축하는 데 주력하고 있음 ✓ 이번 상황은 사이버보안이 단순한 기술적 문제를 넘어 국가 안보와 직결된 지정학적 이슈임을 다시 한번 각인시키는 계기가 됨 ✓ 핵심 인프라의 폐쇄망 운영 및 망 분리 정책의 실효성을 재검토하고 유사시 수동 운영 전환 절차를 점검함 ✓ 사이버 위협에 대한 범국가적 대응 성숙도를 높이기 위해 민·관·군 합동 보안 훈련 실시를 정례화할 계획임 ✓ https://lanotaeconomica.com.co/movidas-empresarial/colombia-en-alerta-por-escalada-de-ciberataques-en-medio-de-tensiones-entre-estados-unidos-e-iran/
[파나마] 디지털 전환·연결성·보안을 파나마 미래의 핵심 열쇠로 정의	▸ **국가 경쟁력 강화를 위한 3대 축으로서의 디지털 정책 추진 방향 제시(3월 29일)**

이 슈	주 요 내 용 및 시 사 점
	✓ 파나마 정부와 산업계 리더들은 디지털 전환, 네트워크 연결성, 사이버 보안을 파나마의 지속 가능한 성장을 위한 3대 핵심 동력으로 설정함 ✓ 파나마 운하와 연결된 물류 허브의 효율성을 높이기 위해 전 공정의 디지털화를 추진하되, 이에 따른 사이버 리스크 관리를 병행함 ✓ 초고속 인터넷 보급을 확대하여 디지털 격차를 해소하고 모든 시민이 안전하게 행정 서비스에 접근할 수 있는 환경을 조성함 ✓ 보안을 디지털 경제의 인프라로 인식하고 국가 사이버 안보 예산을 대폭 확충하여 방어 시스템을 현대화할 계획임 ✓ 글로벌 기술 기업들의 데이터 센터를 유치하기 위해 강력한 데이터 보호법과 안정적인 에너지 공급망 등 최적의 비즈니스 환경을 제공함 ✓ 전문가들은 파나마가 '디지털 허브'로 도약하기 위해서는 기술 도입뿐만 아니라 보안 전문 인력 양성 생태계 조성이 시급하다고 조언함 ✓ 디지털 서비스에 대한 시민들의 신뢰를 확보하기 위해 투명한 거버넌스와 엄격한 보안 인증 체계를 구축하려는 노력이 지속됨 ✓ 이번 비전은 파나마가 지리적 요충지를 넘어 디지털 영토에서도 글로벌 주도권을 확보하겠다는 강력한 의지를 반영함 ✓ 민관 협력을 통해 국가 사이버 위기 대응 로드맵을 정립하고 정기적인 범국가적 보안 훈련을 실시할 예정임 ✓ 차세대 통신 기술인 6G와 양자 보안 등 미래 기술에 대한 연구 투자와 국제 표준 활동 참여를 독려함 ✓ https://www.prensa.com/notas-de-prensa/transformacion-digital-conectividad-y-ciberseguridad-claves-para-el-futuro-digital-de-panama/
[코스타리카] 사이버 위협 대응을 위한 국가 보안 역량 강화 추진	▸ **글로벌 파트너십 기반의 보안 인프라 현대화 및 사고 대응 프로토콜 정립(3월 30일)** ✓ 코스타리카 정부는 최근 증가하는 랜섬웨어 및 국가 배후 해킹 위협에 맞서 범정부 차원의 보안 강화 대책을 수립하고 이행 중임 ✓ 미국 등 우방국과의 전략적 협력을 통해 보안 관제 센터(SOC)의 장비를 현대화하고 전문 인력에 대한 기술 교육을 확대함 ✓ 공공 부문의 디지털 자산을 보호하기 위해 클라우드 기반의 통합 보안 플랫폼을 도입하고 실시간 위협 가시성을 확보하는 데 주력함 ✓ 사이버보안을 국가 안보의 핵심 요소로 규정하고 총리실 직속의 보안 컨트롤 타워 기능을 대폭 강화함 ✓ 사고 발생 시 신속한 복구와 서비스 연속성 보장을 위해 정기적인 재난 복구(DR) 훈련과 데이터 백업 시스템 점검을 의무화함 ✓ 시민들의 보안 의식을 높이기 위한 대국민 캠페인을 전개하고 피싱 및 스캠에 대한 예방 수칙을 적극적으로 홍보함 ✓ 코스타리카 내 주요 기반 시설(전력, 통신, 금융) 운영사들과의 정보 공유 네트워크를 구축하여 위협에 공동 대응하는 체계를 마련함 ✓ 사이버보안 시장의 성장을 지원하기 위해 관련 기술 스타트업 육성과 외국 보안 기업 유치를 위한 인센티브 제공을 검토함 ✓ 국제적인 사이버보안 평가 지표에서 상위권을 기록하기 위해 법적 프레임워크 정비와 기술적 방어 수준을 동시에 끌어올리고 있음 ✓ 이번 조치는 과거 대규모 사이버 공격으로 입은 피해를 교훈 삼아 국가 전반의 디지털 회복 탄력성을 근본적으로 개선하려는 의지를 보여줌 ✓ https://thecostaricanews.com/costa-rica-is-strengthening-its-capabili

이 슈	주 요 내 용 및 시 사 점
	ties-to-address-cyber-threats/
[멕시코] UNODC-Scitum, 사이버 범죄 척결을 위한 파트너십 체결	▸ **국제기구와 현지 보안 기업의 협력을 통한 수사 역량 강화 및 예방 활동 전개(3월 30일)** ✓ 유엔마약범죄사무소(UNODC)와 멕시코 최대 보안 기업인 사이텀(Scitum)은 사이버 범죄 대응 역량을 높이기 위한 전략적 파트너십을 체결함 ✓ 양측은 멕시코 내 수사 기관과 법 집행 공무원들을 대상으로 최신 디지털 포렌식 기술과 사이버 범죄 수사 기법 교육을 실시함 ✓ 특히 아동 성착취물 유통, 다크웹 기반 마약 거래, 온라인 사기 등 고도화되는 사이버 범죄 조직의 활동을 차단하는 데 초점을 맞춤 ✓ Scitum은 자사가 보유한 위협 인텔리전스와 공격 트렌드 분석 데이터를 UNODC에 공유하여 범죄 예방 정책 수립을 지원함 ✓ 이번 협력에는 기업과 일반 시민들을 위한 사이버 보안 인식 제고 캠페인과 예방 가이드라인 배포 활동이 포함됨 ✓ 국제적인 수사 공조 체계를 강화하여 국경을 넘나드는 사이버 범죄자들을 추적하고 처벌하는 효율적인 프로세스를 구축함 ✓ 민간의 기술력과 국제 기구의 거버넌스를 결합하여 멕시코의 사이버 공간을 더욱 안전하게 만들려는 모범적인 협력 사례로 평가됨 ✓ 대학 등 교육 기관과 연계하여 미래의 사이버 수사 전문가를 양성하기 위한 장학 프로그램 및 실습 기회 제공이 논의 중임 ✓ 멕시코 내 중소기업들을 위한 사이버 범죄 예방 툴킷(Toolkit)을 공동 개발하여 무상으로 보급할 계획임 ✓ 이번 파트너십은 멕시코가 국제 사회와 협력하여 사이버 범죄에 단호히 대응하겠다는 강력한 메시지를 전달함 ✓ https://mexicobusiness.news/cybersecurity/news/unodc-scitum-join-forces-fight-cybercrime-mexico
[파나마] 클라우드·보안·AI를 효율적 디지털 정부 구현의 3대 지주로 설정	▸ **행정 서비스의 생산성 향상과 보안성 강화를 위한 기술 통합 로드맵 가동(3월 30일)** ✓ 파나마 정부는 국가 행정의 효율성을 극대화하기 위해 클라우드 컴퓨팅, 사이버보안, 인공지능을 결합한 차세대 디지털 정부 아키텍처를 수립함 ✓ 정부 부처별로 흩어져 있던 IT 자원을 국가 통합 클라우드로 전환하여 운영 비용을 절감하고 보안 관리를 중앙 집중화함 ✓ AI 기술을 행정 업무에 도입하여 데이터 분석 및 의사결정의 정확도를 높이되, AI 모델의 보안성과 데이터 프라이버시 확보를 최우선으로 고려함 ✓ 사이버 보안을 모든 디지털 행정 서비스의 기본 탑재 요소(Built-in)로 설정하여 설계 단계부터 보안성을 검증하는 프로세스를 도입함 ✓ 시민들에게 안전한 비대면 행정 서비스를 제공하기 위해 고도화된 본인 인증 체계와 데이터 암호화 전송 기술을 적용함 ✓ 전문가들은 디지털 정부의 성공은 기술 도입보다 보안 사고에 대한 투명한 대응과 국민의 신뢰 확보에 달려 있다고 조언함 ✓ 정부는 보안 사고 예방을 위해 전 공무원을 대상으로 정기적인 사이버 보안 인식 교육과 모의 피싱 훈련을 실시함 ✓ 클라우드 환경에서의 위협 탐지를 위해 클라우드 보안 태세 관리(CSPM) 및 워크로드 보호(CWPP) 솔루션 도입에 예산을 배정함

이 슈	주 요 내 용 및 시 사 점
	✓ 이번 로드맵은 파나마를 중남미에서 가장 효율적이고 안전한 디지털 정부 모범 사례로 만들겠다는 비전을 담고 있음 ✓ 민간 기술 기업들과의 협력을 통해 공공 부문에 최신 보안 기술을 적기에 도입하고 현지 기업들의 성장을 지원하는 생태계를 조성함 ✓ https://www.laestrella.com.pa/contenido-patrocinado/cloud-ciberseguridad-e-ia-pilares-para-un-estado-mas-eficiente-y-productivo-en-panama-IG21051494
[에콰도르] 국회, 사이버 보안 강화 유기법(Organic Law) 최종 승인	▸ **국가 사이버 안보 체계 제도화를 위한 법적 근거 마련 및 규제 프레임워크 확립(3월 31일)** ✓ 에콰도르 국회는 국가 사이버 안보 역량을 근본적으로 강화하기 위한 '사이버 보안 강화 유기법'을 압도적인 찬성으로 통과시킴 ✓ 이 법안은 국가사이버보안위원회(CNCS) 설립과 국가 침해 사고 대응 센터(CERT)의 권한 강화를 골자로 하며, 범정부 차원의 통합 방어 체계를 구축함 ✓ 공공 기관 및 중요 정보 인프라 운영사들에 대해 정기적인 보안 감사와 위협 보고를 의무화하여 책임 있는 보안 관리를 강조함 ✓ 개인정보 보호 규정을 대폭 강화하고 데이터 유출 사고 발생 시 기업에 부과되는 과징금 및 처벌 수위를 상향 조정함 ✓ 법안에는 사이버 보안 인프라 구축을 위한 예산 확보 방안과 전문 인력 양성을 위한 교육 시스템 도입 근거가 포함됨 ✓ 에콰도르 정부는 이번 법안 통과를 통해 디지털 경제 성장을 지원할 안전한 법적 토대를 마련하고 대외적인 국가 신뢰도를 높이려 함 ✓ 전문가들은 법 제정 자체보다 실질적인 시행령 마련과 현장 이행력이 중요하다며 구체적인 기술 표준 수립을 촉구함 ✓ 민간 부문의 보안 투자 확대를 유도하기 위한 세제 혜택 및 지원 프로그램 운영 근거가 법안에 반영됨 ✓ 국제적인 사이버 범죄 공조 체계에 적극 참여하고 글로벌 보안 표준을 국내에 안착시키기 위한 제도적 장치를 마련함 ✓ 이번 유기법은 에콰도르가 사이버 위협으로부터 국가 주권을 수호하고 디지털 전환을 가속화하는 데 결정적인 역할을 할 것으로 평가됨 ✓ https://ecuadorcomunicacion.com/asamblea-nacional-aprueba-ley-organica-para-el-fortalecimiento-de-la-ciberseguridad
[멕시코] 준비성 격차 해소를 위한 사이버 회복 탄력성 최우선 순위 설정	▸ **급격한 디지털 전환 속도와 보안 대응 역량 간의 불균형 해결을 위한 전략 수립(3월 31일)** ✓ 멕시코 기업 및 정부 기관들이 디지털 전환을 서두르고 있으나, 실제 사이버 공격에 대한 준비성(Readiness)은 여전히 낮은 수준에 머물러 있다는 조사 결과가 발표됨 ✓ 조사에 따르면 대다수 조직이 고도화된 랜섬웨어 공격을 탐지하고 복구하는 데 필요한 기술적 자산과 프로세스가 미비한 것으로 나타남 ✓ 멕시코 정부는 이러한 '준비성 격차'를 해소하기 위해 국가 차원의 사이버 탄력성 강화 전략을 수립하고 공공 및 민간 부문의 참여를 독려함 ✓ 보안 사고 발생 시 핵심 서비스가 중단되지 않도록 하는 '회복 탄력성' 확보를 위해 백업 시스템 고도화와 모의 훈련 실시가 강조됨

이 슈	주 요 내 용 및 시 사 점
	✓ 특히 공급망 보안 강화를 위해 협력사들에 대한 보안 인증을 의무화하고 통합 위협 관리 체계를 구축하는 방안이 추진됨 ✓ 전문가들은 보안 투자가 단순 장비 도입을 넘어 전문 인력 확보와 조직 내 보안 문화 정착으로 이어져야 한다고 조언함 ✓ 멕시코 내 보안 시장은 이러한 수요에 힘입어 통합 보안 관제(Managed Security) 및 AI 기반 자동 방어 솔루션을 중심으로 급성장하고 있음 ✓ 정부는 중소기업들이 최소한의 보안 수준을 갖출 수 있도록 보안 바우처 지원과 기술 가이드라인 보급을 확대할 계획임 ✓ 이번 전략은 멕시코가 라틴아메리카 내 사이버 범죄의 주요 표적이 되고 있는 현실을 타개하기 위한 생존 전략으로 평가됨 ✓ 국가 전체의 사이버 보안 성숙도를 높이기 위해 지표 기반의 성과 관리를 도입하고 정기적인 국가 보안 보고서를 발간할 예정임 ✓ https://mexicobusiness.news/cybersecurity/news/mexico-prioritizes-cyber-resilience-amid-readiness-gap
	▶ 시사점 및 국내 보안 기업 진출 포인트 ✓ 중남미 주요국의 사이버 보안 법제화 및 거버넌스 체계 제도화 본격화 - 칠레의 사이버 보안 프레임워크 법(Ley Marco) 시행과 에콰도르의 사이버보안 강화 유기법 승인은 중남미 국가들이 보안을 법적 규제 영역으로 편입시키고 있음을 보여줌 - 이는 KISA의 정책 협력 네트워크를 통해 한국의 정보보호 관련 법령 및 인증 체계(ISMS 등) 노하우를 전수하고, 국내 보안 컨설팅 기업들이 현지 정부의 제도 설계 및 컴플라이언스 시장에 진출할 수 있는 절호의 기회임 ✓ AI 기반 지능형 위협 증대에 따른 AI 보안 솔루션 및 통합 대응 체계 수요 급증 - 멕시코의 Claude Code 악용 공격 사례와 브라질의 Rust 기반 신종 악성코드 출현은 공격 도구의 지능화와 탐지 회피 기술의 고도화를 증명함 - 국내 보안 기업이 보유한 AI 기반 이상 행위 탐지(XDR), 자동화된 사고 대응(SOAR), 그리고 생성형 AI 보안 위협 차단 기술은 현지 공공 및 금융권의 'AI vs AI' 방어 전략 구축에 핵심적인 솔루션으로 자리 잡을 수 있음 ✓ 국가 핵심 인프라 보호 및 글로벌 기술 협력을 통한 대규모 보안 프로젝트 확대 - 코스타리카 전력공사(ICE)의 사이버 스파이 피해와 파나마 물류 허브 보안 강화 움직임은 국가 핵심 인프라 보호를 위한 폐쇄망 보안 및 OT/ICS 보안 수요를 창출하고 있음 - 영국, 미국, 폴란드 등 선진국과의 전략적 대화가 활발한 만큼, 우리나라도 G2G 협력을 강화하여 한국형 보안 관제 모델과 통합 보안 플랫폼을 패키지화해 중남미 대형 프로젝트 수주에 박차를 가해야 함

KISA 정보보호 해외진출 전략거점(중동아프리카) 3월 주요동향

2026 3 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

[해외 언론]

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 이란 인터넷 마비	**1. 이스라엘-미국 합동 공격에 따른 이란의 '국가적 인터넷 마비' 지속** 2026년 2월 28일 실행된 이스라엘과 미국의 'Roaring Lion' 및 'Operation Epic Fury' 작전의 여파로, 3월 초 이란의 인터넷 연결성이 평상시의 **1~4% 수준**으로 급락하며 사실상 국가 전체가 오프라인 상태에 빠졌습니다. 이 공격은 이란의 정부 서비스, 미디어, 항공 및 에너지 인프라를 타겟으로 한 역사상 최대 규모의 사이버 공격으로 기록되었습니다. **출처:** CloudSEK Situation Report https://www.cloudsek.com/blog/middle-east-escalation-israel-iran-us-cyber-war-2026
[중동전쟁] 에너지 기관 해킹	**2. 'Handala Hack', 사우디 및 이스라엘 에너지 기업 침해 주장** 이란 정보통신부(MOIS)와 연계된 해커 그룹 'Handala Hack'은 3월 초, 이스라엘, 사우디아라비아, 요르단의 주요 석유 및 가스 기관들을 해킹했다고 발표했습니다. 이들은 공격의 증거로 내부 데이터를 공개하며, 중동 지역 내 친서방 국가들의 에너지 인프라를 마비시키겠다는 위협을 가했습니다. **출처:** Industrial Cyber https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran-as-hacktivists-hit-governments-defense-critical-sectors/
[중동전쟁] 랜섬웨어 공격	**3. 의료 기기 거물 'Stryker' 대상 이란계 와이퍼(Wiper) 공격** 미국 CISA는 3월 11일, 글로벌 의료 기술 기업인 스트라이커(Stryker)가 정교한 사이버 공격을 받아 대량의 기업용 단말기 데이터가 삭제되었다고 확인했습니다. 이 공격은 이란과 연계된 위협 조직의 소관으로 추정되며, 단순한 랜섬웨어가 아닌 데이터를 영구 파괴하는 '와이퍼' 악성코드가 사용된 것으로 분석되었습니다. **출처:** Industrial Cyber / CISA Alert https://industrialcyber.co/cisa/cisa-flags-rising-threats-to-endpoint-management-systems-after-stryker-breach-urges-stronger-defense/

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 이스라엘 공습 경보 앱 악설 파일 유포	**4. 이스라엘 'RedAlert' 앱 사칭 스파이웨어 유포** 팔로알토 네트웍스(Unit 42)는 3월 26일 보고서를 통해, 이스라엘 국민들이 사용하는 공습 경보 앱 'RedAlert'을 모방한 악성 안드로이드 설치 파일(APK)이 유포되고 있다고 경고했습니다. 이 가짜 앱은 설치 시 사용자의 위치 정보, 연락처, 메시지를 탈취하고 마이크를 통해 주변 소리를 도청하는 기능을 수행합니다. **출처:** Palo Alto Networks Unit 42 https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 주요 정부 및 군사 대상 DDoS 공격	**5. 'UniT 313' 그룹, 바레인 및 사우디 정부군 대상 DDoS 공격** 이란계 해킹 조직 'UniT 313'은 3월 초순, 미국과 이스라엘의 군사 작전을 지원하는 바레인과 사우디아라비아의 주요 정부 및 군사 웹사이트를 대상으로 대규모 DDoS 공격을 감행했습니다. 이로 인해 일부 대국민 서비스 포털이 수 시간 동안 마비되었으며, 이는 물리적 전쟁에 대응하는 심리전의 일환으로 해석되었습니다. **출처:** Industrial Cyber Reports https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran/
[중동전쟁] 미국 금융 다상 사이버 공격	**6. 미국 금융 기관 대상 이란의 '보복성' 사이버 침입 시도 증가** FINRA와 FBI는 3월 16일 합동 경보를 통해, 이란 국적의 위협 행위자들이 미국 금융 서비스 부문과 주요 인프라를 타겟으로 자격 증명 탈취 및 브루트 포스(무차별 대입) 공격을 강화하고 있다고 발표했습니다. 특히 클라우드 기반 관리 도구의 취약점을 노린 침투 시도가 급증한 것으로 파악되었습니다. **출처:** FINRA Cybersecurity Alert https://www.finra.org/rules-guidance/guidance/cybersecurity-alert-heightened-threats-iranian-cyber-actors

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 가짜 도메인 등록	**7. 중동 분쟁 테마 피싱 도메인 7,000여 개 대량 생성** 3월 한 달 동안 '중동 긴장 상태'나 '전쟁 구호'를 테마로 한 가짜 도메인 7,381개가 새롭게 등록된 것으로 조사되었습니다. 공격자들은 이 도메인들을 활용해 기부금을 가로채거나, 기업 ERP 시스템으로 위장한 피싱 페이지를 운영하여 글로벌 공급망 기업들의 계정 정보를 탈취했습니다. **출처:** Unit 42 Threat Brief https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 이스라엘 통신업체 공격	**8. 이스라엘 광통신 업체 대상 '사이버 이슬람 저항군'의 공격** 'Cyber Islamic Resistance'라고 자칭하는 그룹은 3월 초, 이스라엘의 광섬유 통신 제공업체와 연결된 가정용 라우터 및 산업용 제어 시스템(ICS) 제조사를 침해했다고 주장했습니다. 또한 미국 군사 온라인 디렉토리에 대한 서비스 거부 공격을 수행하여 미군 관련 정보 접근을 방해했습니다. **출처:** Industrial Cyber https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran/
[중동전쟁] 이스라엘, 이란 정보 탈취	**9. 'Anonymous' 그룹의 이란 혁명수비대(IRGC) 정보 유출** 친이스라엘 해커 그룹인 'Anonymous - אנונימי'는 3월 중순, 이란 혁명수비대원 및 군 작전 요원들의 개인 신상 정보(PII)를 탈취해 온라인에 공개했습니다. 이는 이란의 사이버 공세에 대한 맞대응으로, 적대 진영 요원들의 신분을 노출시켜 심리적 압박을 가하는 전략을 사용했습니다. **출처:** Industrial Cyber Reports https://industrialcyber.co/reports/cyber-retaliation-surges-after-us-israel-strikes-on-iran/

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 미국 엔드포인트 보안 강화	**10. 미국 CISA, 엔드포인트 관리 시스템 취약점 긴급 업데이트** 3월 19일, CISA는 중동 지역 긴장 고조에 따라 이란 연계 조직들이 기업의 '엔드포인트 관리 소프트웨어'를 악용하여 대규모 파괴 공격을 감행하고 있다고 경고했습니다. 특히 마이크로소프트 인튠(Intune) 등 관리 도구를 통한 악성코드 배포를 막기 위한 다중 인증(MFA) 강화 지침을 발표했습니다. **출처:** Industrial Cyber / CISA https://industrialcyber.co/cisa/cisa-flags-rising-threats-to-endpoint-management-systems-after-stryker-breach-urges-stronger-defense/
[중동전쟁] 이란 은행 피칭 증가	**11. 이란 은행 시스템 마스크퀘레이딩(Masquerading) 공격** 3월 하순, 이란 내 인터넷 복구 시점에 맞춰 이란의 주요 은행을 사칭한 가짜 모바일 앱과 피싱 사이트가 급증했습니다. 이는 이스라엘 혹은 친서방 해커들이 금융 혼란을 가중시키기 위해 수행한 것으로 보이며, 시민들의 뱅킹 자격 증명을 가로채어 경제적 불안을 조장했습니다. **출처:** Unit 42 (March 26 Update) https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 사우디 정유시설 하이브리드 사이버공격	**12. 사우디 동부 에너지 시설 대상 사이버 물리 시스템(CPS) 경보** 3월 3일 다란 지역에 대한 물리적 무인기 공격 위협과 동시에, 사우디 국가사이버보안국(NCA)은 인근 정유 시설의 제어망에 대한 비정상적인 트래픽 침투를 감지하고 최고 단계 경보를 발령했습니다. 이는 물리적 타격과 사이버 교란을 병행하는 전형적인 중동식 하이브리드 공격 패턴을 보였습니다. **출처:** U.S. Embassy Riyadh / NCA Alerts https://sa.usembassy.gov/security-alert-threat-of-imminent-missile-uav-attacks-over-dhahran-mar-3-2026/

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 글로벌 IT 솔루션 기업들의 내부 이메일 유출	**13. 'APT Iran', 글로벌 기업 대상 해킹 및 유출 (Hack-and-Leak) 재개** 3월 26일, 이란 정보부와 연결된 'APT Iran' 그룹이 중동 국가들과 협력하는 글로벌 IT 솔루션 기업들의 내부 이메일을 유출하기 시작했습니다. 인터넷 차단으로 활동이 일시 위축되었으나, 외부 인프라를 활용해 이스라엘과의 협력 관계가 있는 기업들을 압박하는 활동을 지속하고 있습니다. **출처:** Unit 42 Threat Intelligence https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 사우디 네트워크장비 취약점 공격에 활용	**14. HPE 및 시스코(Cisco) 인프라 타겟 치명적 취약점 악용** 3월 25일과 31일, 사우디 CERT는 HPE와 시스코 시스템즈의 주요 서버 및 네트워크 장비에서 '치명적(Critical)' 등급의 취약점이 실제 공격에 활용되고 있음을 보고했습니다. 중동 분쟁의 당사자국들이 서로의 국가 통신망을 마비시키기 위해 제로데이 취약점을 공격적으로 소모하고 있는 양상이 확인되었습니다. **출처:** National Cybersecurity Authority (NCA) https://nca.gov.sa/en/cert/7496/
[중동전쟁] UAE, 이스라엘 금융 대상 피싱 급증	**15. UAE 금융권 대상 AI 기반 피싱 공격 급증** 체크포인트(Check Point)는 3월 보고서에서 UAE와 이스라엘의 금융 기관을 대상으로 AI를 활용해 정교하게 번역된 아랍어·히브리어 피싱 메일이 3월 중순부터 500% 이상 증가했다고 밝혔습니다. 공격자들은 가짜 은행 통지서를 발송해 실시간 결제 시스템의 권한을 탈취하려 했습니다. **출처:** KBI Media / Check Point Research https://kbi.media/press-release/check-point-softwares-2026-cyber-security-report/

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 캐나다 내 유대인 관련 사이버 공격 경고	**16. 캐나다 사이버 보안 센터, 중동발 사이버 위협 경보 발령** 3월 2일, 캐나다 정부는 중동 지역의 물리적 충돌이 캐나다 내 유대인 커뮤니티와 에너지 기업에 대한 사이버 보복으로 이어질 수 있다고 경고했습니다. 특히 이란계 해커들이 원격 접속 툴을 이용해 서방 국가의 수처리 시설과 전력망을 타겟으로 삼는 움직임을 포착했습니다. **출처:** Canadian Centre for Cyber Security https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026
[중동전쟁] 악성코드 감염 시도 증가	**17. StealC 인포스틸러, 중동 지역 내 전례 없는 살포** 3월 한 달 동안 중동 지역의 정부 관료와 언론인을 타겟으로 한 'StealC' 악성코드 감염 시도가 빈번하게 발생했습니다. 이 스파이웨어는 브라우저에 저장된 비밀번호, 메신저 세션, 가상화폐 지갑 정보를 즉시 탈취하며, 이는 분쟁 중 첩보 활동의 일환으로 분석되었습니다. **출처:** Unit 42 Global Threat Intelligence https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 이란의 사망 위협 메일 배포	**18. 이란 배후 'Handala Hack'의 미국 인플루언서 협박 메일** 3월 하순, 이스라엘에 우호적인 입장을 표명한 미국과 캐나다의 주요 정치·사회 인플루언서들이 'Handala Hack'으로부터 사망 위협을 포함한 협박 이메일을 받았습니다. 이는 사이버 공간에서의 심리 전술이 온라인 침해를 넘어 오프라인 개인의 신변 안전을 위협하는 수준으로 확장되고 있음을 보여줍니다. **출처:** Unit 42 (March 26 update) https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[중동전쟁] 두바이 정부 사칭 피칭 증가	**19. 두바이 정부 당국 사칭 사회공학적 기금 사기** 3월 말, 공격자들은 두바이 정부 기관을 사칭하여 전쟁 피해자들을 돕기 위한 긴급 구호 기금을 모금한다는 명목으로 가짜 웹사이트를 운영했습니다. 이는 인도적 지원을 사칭해 암호화폐와 신용카드 정보를 탈취하는 파렴치한 사이버 범죄 사례로 기록되었습니다. **출처:** Palo Alto Networks / Unit 42 https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] 이란의 사이버공격 보복 경고	**20. 이란의 사이버 작전 복구 및 파괴적 공격 위험 고조** 3월 26일 기준, 이란의 인터넷 차단이 27일째 이어지고 있는 가운데, 전문가들은 이란이 외부망 연결을 복구하는 즉시 서방의 주요 타겟을 향해 매우 강력하고 파괴적인 '최후의 한 방(Destructive Attacks)'을 준비하고 있을 가능성이 크다고 경고했습니다. **출처:** Unit 42 Threat Analysis https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

[국내 언론]

이 슈	주 요 내 용 및 시 사 점
[중동전쟁] AI와 사이버보안 기술 활용 공격	**1. 중동 분쟁, AI 무기 및 사이버 보안의 '잔혹한 시험장'** 보안뉴스는 2026년 3월 빅데이터 분석 결과를 통해, 이스라엘과 이란의 중동 분쟁이 '군사 AI'와 사이버 보안 기술의 시험장이 되고 있다고 분석했습니다. 이스라엘의 '라벤더(Lavender)' 시스템 등 AI를 활용한 표적 식별 기술이 실전에 도입되면서, 이에 따른 '데이터 오염' 공격 및 사이버 보안 리스크가 현대전의 핵심 변수로 떠올랐습니다. 기사는 인간의 통제를 벗어난 AI 자율성과 사이버 취약점 극복이 인류의 시급한 과제임을 강조했습니다. **출처:** 보안뉴스 (2026.04.01 – 3월 분석 기사) https://www.boannews.com/media/view.asp?idx=142962
[중동전쟁] 이란의 사이버보복 급증	**2. 이란의 '사이버 보복' 급증 및 국가 기간시설 위협** 3월 하순, 이란은 이스라엘과 미국의 군사 압박에 대응하여 '걸프국 생명줄을 끊겠다'는 초강경 선언과 함께 대대적인 사이버 및 미사일 도발을 감행했습니다. 한국 언론은 이 과정에서 사우디아라비아와 UAE 등 걸프 국가들의 에너지 시설 및 통신망에 대한 이란계 해커들의 침투 시도가 빈번해지고 있음을 보도했습니다. 특히 호르무즈 해협 인근의 물류 차질과 연계된 하이브리드 공격 양상에 대해 한국 경제에 미칠 영향을 우려하며 비중 있게 다루었습니다. **출처:** KBS 뉴스 (2026.03.22 / 03.25) https://www.youtube.com/watch?v=pj_JsH6T4Lo

[중점 키워드 및 시사점]

No.	키워드	주요 내용 및 시사점
1	국가적 인터넷 마비	이스라엘·미국의 'Roaring Lion' 작전으로 이란 인터넷이 평시의 1~4%로 급락. 국가 인프라 전체를 오프라인화하는 **역대 최대 규모의 사이버전** 사례 기록.
2	에너지 인프라 침해	'Handala Hack'이 사우디·이스라엘 에너지 기업 해킹 주장. 지정학적 적대국뿐만 아니라 **친서방 국가의 기간 시설**까지 공격 범위 확대.
3	와이퍼(Wiper) 공격	미 의료기기 기업 'Stryker' 대상 데이터 영구 파괴 공격 발생. 금전 목적의 랜섬웨어를 넘어 **데이터를 완전히 삭제하는 파괴적 공격** 양상 강화.
4	스파이웨어 유포	공습 경보 앱 'RedAlert' 사칭 APK 유포. 국민의 생존과 직결된 **공공 서비스 앱을 사칭**하여 도청 및 민감 정보를 탈취하는 치밀한 사회공학적 기법 사용.
5	보복성 DDoS	'UniT 313'의 바레인·사우디 정부군 공격. 물리적 군사 작전을 지원하는 국가들에 대해 **심리적 압박과 서비스 마비**를 시도하는 하이브리드전 양상.
6	금융권 침입 시도	이란계 해커들의 미 금융 부문 브루트포스 공격 강화. 특히 **클라우드 기반 관리 도구의 취약점**을 노린 침투가 급증하여 클라우드 보안 관리의 중요성 대두.
7	분쟁 테마 피싱	중동 긴장 테마 가짜 도메인 7,000여 개 등록. 전쟁 구호를 명목으로 **글로벌 공급망 기업의 자격 증명 탈취**를 노리는 피싱 캠페인 대대적 전개.
8	라우터 및 ICS 공격	'사이버 이슬람 저항군'의 이스라엘 광통신 업체 및 제어시스템(ICS) 침해. **가정용 라우터까지 공격 대상**에 포함하여 민간과 산업망을 동시에 위협.
9	신상 정보 유출	'Anonymous'의 이란 혁명수비대(IRGC) 요원 정보 공개. 적대 진영 요원의 **개인 신상을 노출**시켜 군사 작전 수행 능력을 저해하는 맞대응 전략 실행.
10	엔드포인트 보안	CISA의 관리 소프트웨어 패치 긴급 명령. 이란 연계 조직이 **기업용 관리 도구(Intune 등)를 악용**하여 파괴적 코드를 유포하는 것에 대한 강력 경고.
11	마스크쿼레이딩	이란 내 인터넷 복구 시점에 맞춘 가짜 은행 앱 유포. 서비스가 재개되는 혼란을 틈타 **금융 대란을 유도**하고 시민의 경제적 불안을 가중시킴.
12	하이브리드 공격 패턴	사우디 다란 지역의 물리적 드론 공격과 사이버 침투가 동시에 발생. **물리적 타격과 사이버 교란이 병행**되는 현대적 분쟁 모델의 전형을 보여줌.
13	Hack-and-Leak	'APT Iran'의 글로벌 IT 기업 내부 이메일 유출. 국가 차원의 차단에도 불구하고 **외부 인프라를 활용**해 이스라엘 협력 기업들에 대한 압박 지속.
14	인프라 취약점 소모전	HPE·시스코 등 핵심 장비의 제로데이 취약점 악용. 국가 간 통신망 마비를 위해 **치명적 취약점을 공격적으로 소모**하는 고도화된 기술전 전개.
15	AI 기반 피싱	UAE·이스라엘 금융권 대상 **AI 생성 정교한 피싱 메일** 500% 급증. 언어 장벽을 극복한 AI 기술이 사이버 범죄의 효율성을 극대화하고 있음을 시사.
16	글로벌 위협 전이	캐나다 등 중동 외 지역으로 사이버 위협 확산. 중동 분쟁의 여파가 **서방 국가의 수처리·전력망 등 기간 시설**까지 전이될 수 있다는 경보 발령.
17	정보 탈취(StealC)	정부 관료 및 언론인 대상 인포스틸러(StealC) 살포. 분쟁 상황에서 **실시간 첩보 수집과 계정 탈취**를 위한 스파이웨어 공격이 전례 없는 수준으로 발생.
18	개인 신변 협박	미 인플루언서 대상 협박 메일 발송. 사이버 공격이 시스템 침해를 넘어 **특정 여론 형성층에 대한 물리적 위협**과 심리전으로 확장되는 추세.
19	구호 기금 사기	두바이 정부 사칭 구호 기금 모금 사기 웹사이트 운영. 인도적 위기 상황을 악용해 **암호화폐와 금융 정보를 탈취**하는 비윤리적 범죄 기승.
20	파괴적 공격의 전조	전문가들이 분석한 이란의 '최후의 한 방' 가능성. 인터넷 복구 이후 서방 인프라를 향한 **대규모 파괴적 공격(Destructive Attacks)**의 위험성 고조.