KISA 정보보호 해외진출 전략거점(동남아) 1월 주요동향

2023. 1. 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
말레이시아 개인정보 유출	▸ **Astro, Maybank 및 SPR의 1,300만 말레이시아 사용자 데이터 유출** ✓ 유출된 데이터가 암시장에서 거래되고 있다는 내용의 트윗이 말레이사 통신 및 멀티미디어부 장관 Fahmi Fadzil에게 발송 ✓ 유출된 사용자 데이터는 MyKad 번호, 주소, 전화번호를 포함 ✓ 통신 및 멀티미디어부 장관은 지난 6년 동안 데이터 유출로 벌금을 부과 받은 회사는 20개에 불과하며 평균 RM 24,000 벌금을 부과하였다고 발표하였음 ✓ 장관은 벌금이 너무 낮은 수준이며 데이터 보호와 관련된 법률을 검토할 계획임을 발표
인도네시아 정부 첫 번째 데이터 센터 개소	▸ **인도네시아 첫 번째 데이터 센터가 중부 자바에 1월 3일 개소** ✓ 첫 번째 정부 데이터 센터로 BSSN에 등록할 예정 ✓ 중앙 자바 주지사 Ganjar Pranowo는 날씨, 지역, 식물, 유형, 파종 시간 및 수확 등 농업 부문을 예로 들며 모든 분야와 정부, 지방 및 시/군에서 사용되는 데이터를 이전할 계획임
태국 개인정보 보호를 위한 포털 정부 플랫폼 구축	▸ **태국은 PDPA 규정 준수를 위한 정부 플랫폼(GPPC)을 구축하여 정부 예산 절약 예정** ✓ 데이터 보호법이 공공 및 민간 부문의 사업을 관장하는 중심법이 되었음을 강조하며 개인 데이터 수집, 사용 또는 공개와 관련된 모든 활동은 개인 데이터 보호법을 준수하여야 함 ✓ 현재 국제 플랫폼에 의존하고 있어 예산을 낭비하고 있으며 이를 절약하기 위하여 자국의 개인정보 정부 플랫폼을 구축할 계획이며 이는 국가 디지털 경제 및 사회 위원회의 승인을 득함 ✓ 개인 데이터 보호 위원회(SorSorSor)와 국가 디지털 경제 및 사회 위원회(NorSorChor)이 정부 플랫폼을 개발하고 홍보하는 임무를 수행할 예정 ✓ 자국의 플랫폼이 개발되면 년간 50억 바트 이상을 절약할 수 있을 것으로 예상 ✓ 정부 플랫폼은 개인 데이터 보호에 대한 지식과 이해를 높이기 위한 활동과 전 세계적으로 규정 준수를 모니터링하고 감독하기 위한 지침과 프로세스를 제공
	▸ **시사점** ✓ 동남아 권역 내에서도 개인정보보호는 끊임없는 이슈이며, 개인정보보호 유출에 따른 법제도 마련 및 개선 등 대응방안이 필요 ✓ 관련하여 한국의 우수한 개인정보보호 제도 및 대응 사례 소개, 기업 진출 연계 등 추진 가능

KISA 정보보호 해외진출 전략거점(북미) 1월 주요동향

2023. 1. 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[미국] 보안 전문가에 대한 수요는 계속 높을 것이지만 경제적 여파로 고용이 더욱 어려워질 것	▸ **경제적 역풍은 사이버보안 기술 부족을 심화시킬 수 있음** ✓ ESG와 ISSA(Information System Security Association International)의 최신 연구 보고서에 따르면 조직의 57%가 글로벌 사이버 보안 기술 부족의 영향을 받았다고 주장하는 반면 조직의 44%는 기술 부족이 악화되었다고 생각 **인력이 가장 부족한 사이버 보안 역할** ✓ 인력이 가장 부족한 직업은 2022년 후반부터 ESG 리서치에 따르면 아래와 같음 ✓ 조직의 37%는 보안 설계자가 부족하며, 이러한 부족은 클라우드 보안 설계자와 기술 통합에 중점을 둔 영역에서 심각함 ✓ 조직의 35%는 보안 엔지니어가 부족하며, 보안 엔지니어는 보안 솔루션을 설치, 구성 및 유지 관리하는 사람들이므로 보안 엔지니어의 부족은 보안 기술을 차선책으로 사용하는 것과 같음 ✓ ESG는 또한 탐지 엔지니어링에 숙련된 개인에 대한 수요가 증가하고 있음을 보고 있음 ✓ 따라서, Anvilogic, CadinalOps 및 SOC Prime과 같은 벤더의 확산은 탐지 엔지니어링 격차를 해소하는 것을 목표로 함 ✓ 조직의 34%는 계층 3 SOC 분석가가 부족하며, 이들은 가장 경험이 풍부한 SOC 분석가로서 어려운 에스컬레이션/조사를 방고 종종 사전 예방적 위협 사냥을 담당함 ✓ 계층 3 분석가 대신 조직은 제너럴리스트에게 전문적인 작업을 요청하는 것 외에는 선택의 여지가 없음 ✓ 조직의 33%는 취약성 관리 분석가가 부족하며, 여기서 부족은 IT 자산이 발견되지 않고 잘못 구성되고 취약한 상태로 남아 있어 사이버 위험을 증가시킴 ✓ 조직의 31%는 CISO, BISO 또는 기타 고위 사이버 보안 직위가 부족하며, 이러한 부족은 많은 조직이 사이버 위험을 식별하고, ✓ 기업 보안 프로그램을 관리하며 경영진과 협력하여 보안을 비즈니스에 맞추는 데 필요한 리더십 없이 보안 프로그램을 운영하고 있음 **경제 침체가 사이버 보안 부족을 악화 시키는 이유** ✓ 우리는 수년 동안 사이버 보안 기술 부족을 처리해 왔지만 여기에 약간의 새로운 주름이 있으며, 바로 현재 경제 상태임 ✓ 향후 12~18개월 동안 경제적 역풍은 사이버 보안 기술 부족의 영향을 악화 시킬 것임 **1. 사이버 보안 전문가는 직업 구하기에 대해 더 까다로울 것임** ✓ 지난 10년 동안 보안 전문가들은 종종 스톡옵션과 연계된 관대한 보상 패키지를 제공 받았음 ✓ 시장이 침체되고 IPO가 보아지 않는 지금, 보안 전문가들은 냉정한 현금을 위해 주식을 기피할 것임 ✓ 단순한 보상을 넘어 경제적 혼란은 더 많은 위험 회피 행동을 유발하는 경향이 있음

이 슈	주 요 내 용 및 시 사 점
	✓ 사이버 보안 전문가는 쪼그리고 앉아 경력 발전에 신중한 접근 방식을 취하고 경제적 폭풍이 사라질 때까지 기다릴 것임 ✓ 이러한 행동 변화는 위험한 경력 이동과 평등이 표준 운영 절차인 실리콘 밸리에서 가장 많이 느낄 수 있음 **2. 보안 서비스 사용이 증가하면 인재 풀이 고갈됨** ✓ 모든 사람의 연구를 보면 더 많은 조직이 과중하고 기술이 부족한 내부 보안 직원을 보강하기 위해 관리형 서비스로 전환하고 있음 ✓ 예를 들어 보안 운영에 대한 최근 ESG 연구에 따르면 조직의 85%가 특정 유형의 관리형 탐지 및 대응(MDR) 서비스를 사용하고 있으며 88%는 향후 관리형 서비스 사용을 늘릴 계획 ✓ 이 패턴이 계속되면 MSSP(Managed Security Service Provider)는 증가하는 수요를 처리하기 위해 인력을 추가해야 함 ✓ 서비스 공급자 비즈니스 모델은 자동화를 통한 확장 작업을 기반으로 하기 때문에 직원 생산성에 대한 더 높은 수익을 계산하고 일반 조직보다 더 많은 보상을 기꺼이 제공할 것임 ✓ 작은 도시에 있는 한 공격적인 보안 서비스 회사는 지역 인재를 거의 독점할 수 있음 ✓ 경영진 수준에서는 가까운 시일 내에 보안 프로그램을 만들고 관리하기 위한 가상 CISO(vCISO) 서비스에 대한 수요가 증가 할 것임 **3. 고용 동결은 방해가 될 것임** ✓ 경기 침체기에 조직은 종종 교육 삭감, 인력 감축 또는 모든 신입 직원 동결과 같은 가혹한 포괄적 결정을 내림 ✓ 이런 일이 발생하면 CISO는 필요한 각 개인을 고용가기 위해 HR과 싸워야 하며 고용 프로세스가 느려지고 조직이 인력이 부족하거나 중요한 기술이 부족함에도 불구하고 보안을 관리해야 함 ✓ 경제적 역풍은 CISO, 특히 이미 보안 인력 및 기술 문제를 다루고 있는 CISO의 작업을 어렵게 하고 있음
[미국] 기업들 사이에서 피싱 및 맬웨어 위협의 증가는 글로벌 사이버 보안 시장 성장을 주도	▸ **2030년까지 6,570억 2,000만 달러 규모로 성장할 글로벌 사이버 보안 시장** ✓ Next Move Strategy Consulting이 발간한 보고서에 따르면 전 세계 사이버 보안 시장 규모는 2021년 1,974억 4,000만 달러이었으며 2030년에는 6,570억 2,000만 달러에 달할 것으로 예상됨 ✓ 이 연구는 업계의 변화하는 시장 역할을 강조할 수 있는 동인, 제약 및 기회에 대한 자세한 분석을 제공함 ✓ 또한 이 연구는 가장 빠르게 성장하고 가장 높은 수익을 창출하는 세그먼트를 결정하기 위해 주요 세그먼트 및 해당 하위 세그먼트에 대한 광범위한 분석을 제공 ✓ 이 보고서는 동인, 제한 요인 및 기회를 기반으로 사이버 보안 산업 역할에 대한 포괄적인 분석을 제공함 ✓ 바이러스 및 트로이 목마를 포함한 맬웨어는 사이버 범죄가 전체 전자 정보 네트워크에 침투, 장악 및 손상을 크게 증가시켜 사이버 보안 보험의 성장을 주도했음 ✓ 높은 비용과 사이버 보안 전문가의 무족은 시장 성장을 억제하며, Next Move Strategy Consulting의 ICT 및 미디어 수석 분석가는 “AI와 함께 블록체인 기술의 도입은 향후 몇 년 동안 시장에 새로운 기회를 창출할 것으로 기대됨”이라고 말함

이 슈	주 요 내 용 및 시 사 점
	✓ 북미는 2021년에 가장 높은 사이버 보안 시장 점유율을 차지했으며, 예측 기간 동안 시장을 지배할 것으로 예상됨 ✓ 이는 기술 발전과 시장 성장을 주도하는 정부의 높은 지출로 인해 국방 및 의료를 포함한 다양한 산업에서 클라우드 기반 솔루션의 사용 증가와 같은 요인에 기인함 ✓ 한편, 아시아 태평양 지역은 다양한 주변 국가의 맬웨어 활동 및 피싱을 포함한 외부 위협이 증가함에 따라 예측 기간 동안 사이버 보안 시장 동향에서 꾸준히 성장할 것으로 예상됨 ✓ 사이버 보안 시장 분석은 세그먼트를 기반으로 각 지역 및 해당 국가에 대한 분석을 제공하여 사이버 보안 산업에 입지를 통합하기 위해 취해야 할 단계를 설명 ✓ 이 분석은 또한 가장 높은 수익 창출 및 가장 빠르게 성장하는 세그먼트를 결정하고 그에 따라 다음 단계를 수행하는 데 도움이 됨
	▶ **시사점** ✓ 경제적 역풍으로 인해 사이버 보안 시장 및 보안 직업에 대한 어려움이 시작될 것으로 예상 됨 ✓ 따라서 대한민국에서도 이에 대한 대비를 해야 하며, 이에 대한 대응을 제대로 하지 못하면 해커들에게 큰 표적이 될 수 있음 ✓ 2030년까지 6,570억 달러 규모로 사이버 보안 시장이 성장할 것으로 예상되며, 특히 북미 시장에서의 성장이 클 것으로 기대 됨 ✓ 이에 대해 꾸준한 기술 개발 및 사이버 보안 시장에 참여하여 우리 기업의 수출 증대 및 세계 시장에서 기술적으로 이끌어 갈 수 있도록 노력해야 함

KISA 정보보호 해외진출 전략거점(아프리카) 1월 주요동향

2023. 1. 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[나이지리아] '23 사이버 보안에 대한 위협 증가 예상	▸ **당국 사이버위협이 증가 예상(나이지리아 사이버보안전문가 협회, '23)** ✓ 사이버 위협의 세계적 감소 추세와 다르게, 당국 사이버보안 악화 예상 * 사이버보안 관련 정부 대응 미흡, IT인프라 노후화 등 다양한 악화 요인 有 ✓ '23 총선, 경제 상황, 보안 위반 보고의 투명성 부족 등에 대비하기 위한 사이버 대응 권고 ✓ 악의적 사용을 위한 정부기관의 컴퓨팅 리소스 악용 사례 예상 및 관련 데이터 유출 방지를 위한 정부 차원 보호 권고
[르완다] 공공 서비스 디지털화 등을 위한 국제 지원 확보	▸ **공공 서비스 디지털화 및 드론 산업 활성화를 위한 지원 확보** ✓ 르완다 정부의 공공 서비스 디지털 전환 및 드론 산업 발전을 위한 국제 지원 확보 * 르완다 정부는 프랑스 개발청(AFD)로부터 3,700만 유로 대출 지원 약정 ✓ 본 지원은 경제적 변화 정책에 따라 공공 및 민간 부문의 서비스 개선 및 만족도 증진 목표 ✓ 중앙 및 지방 정부의 오래된 IT인프라 재구축들을 통한 데이터 활용 가능성 예상
[세이셸] 사이버보안 강화를 위한 범죄수사대 구성 및 인터폴 공조 강화	▸ **세이셸 사이버범죄수사대 설치를 위한 인터폴 공조 협조 요청** ✓ 온라인에 만연한 사이버 사기 및 데이터 유출 등 범죄에 대응하기 위한 정부 조직 필요 ✓ 본 정부 조직 창설 관련 인터폴 협조 요청하였고 사이버보안 대응책 마련 관련 정책 강화 시작 * 세이셸 사이버범죄법 마련('21)에 따라 해당 정부 조직 구성 현실화 ✓ 본 조직 구성의 인적 자원 구성을 위한 프레임워크 작업 및 전문성 극대화를 위한 국제적 지원과 해당 교육 지원 요청 中
[시에라리온] 당국 정보부의 디지털 전환 프로젝트 시행 개시	▸ **World Bank 지원을 통한 디지털 전환 프로젝트 구현 개시** ✓ 시에라리온 정보통신부는 디지털 전환 프로젝트(5년 예정)을 위한 WB 지원 확보 발표 * 디지털 기술 향상 및 정부 디지털 서비스 확대를 위한 지원금(5천만불) 확보 ✓ 정부 디지털 전환은 국가 차원의 서비스 투명성 및 효율성 제고를 위한 혁신적 IT기술 활용의 초석이며, 공공으로부터의 가치 창출로 개선된 서비스 제공 예상 ✓ 디지털 전환을 통한 공공 플랫폼 서비스 향상으로 정부 서비스 접근성 향상 목표
	▸ **시사점** ✓ 아프리카 국가는 중앙집권적 정책 발현을 위한 방안으로 사이버보안 강화를 표명하고, 관련 인프라 및 교육 확충을 위한 대내외 지원 요청 中 ✓ 사이버보안 강화 정책을 위한 국내 정보보호 기업의 진출이 확대 예상되며, 본원에서는 각 국가 대상 국내 기업 소개를 위한 가교 역할 필요

KISA 정보보호 해외진출 전략거점(중남미) 1월 주요동향

2023. 1. 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[푸에르토리코] 사이버 범죄관련 CoE(유럽평의회) 부다페스트 협약 가입	▸ **푸에르토리코 PRITS, 정부의 '22년 디지털 정책 평가** ✓ 푸에르토리코 정부의 혁신 기술 서비스 사무소(PRITS)가 '22년 정부의 디지털 시스템과 플랫폼을 강화하기 위한 프로젝트 및 정책 등을 평가 **<PRITS>** 푸에르토리코 정부(카리브해 위치한 미국의 자치령)의 과학, 기술 및 혁신에 대한 사회 경제적 개발 모델을 구현하기 위해 '19.7.25일 법률 75 기반 '푸에르토리코 혁신 기술 서비스(PRITS)' 설립 목표 : PRITS은 혁신, 기술 및 협업 접근 방식을 통해 푸에르토리코 정부의 디지털 혁신을 주도함과 동시에 국민의 안전을 보장 비전 : 새로운 기술과 세계적 수준의 혁신을 통해 중앙 집중화되고 민첩하며 투명한 대국민 서비스를 효율적으로 개발 사이버 보안 : '21년 2월 1일, 최고 사이버 보안 책임자(CISO)의 고용과 함께 사이버 보안 업무를 공식화하였으며 동 사무소는 연방 기관 및 외부 서비스 제공 업체와의 협력 계약을 통해 푸에르토리코 정부에 중앙 집중식 사이버 보안 서비스를 제공 ✓ PRITS는 "정부 인프라와 정보 시스템이 적절한 보안 통제를 한다" 목표는 전체 인구가 쉽고 용이하게 접근하고 사용할 수 있는 플랫폼 및 애플리케이션 개발의 기반을 만드는 것"에 중점을 뒀다고 설명 ✓ '22.5월, 전체 서비스 보안 운영 센터(SOC)가 기관의 중앙 집중식 사이버 보안 이벤트 모니터링과 함께 출범하였으며 동 모니터링에는 네트워크 및 사용자 계정의 의심스러운 활동에 대한 경고와 장치에 대한 공격에 대한 검색과 보호가 포함 ✓ SOC의 다중 상태 정보 공유 분석 센터 (MS-ISAC)와 760만 달러의 투자를 통해 사이버 공격으로부터 24/7/365 모니터링 서비스와 컴퓨터 및 서버 보호 가능 ✓ 동 서비스 구현 이후, 600건 이상의 사이버 공격이 확인 및 차단되었으며 Autoexpreso, 입법 서비스 사무소 및 Vega Alta 지방 자치 단체의 운영에 영향을 미치는 랜섬웨어와 함께 고속도로 당국의 사고에 대응하여 지원이 제공 ✓ PRITS은 사고에 대한 탐지 및 대응을 위해 미 연방 수사국(FBI), 사이버 보안 및 인프라 국(CISA) 및 공공 안전부(DSP)와 같은 당국의 협력을 받고 있으며 이러한 모든 조치는 사이버 위협을 탐지하고 대응하는 능력을 향상 시킴. 또한, 2023년까지 PRITS는 전년도보다 더 많은 사이버 보안 사고를 식별할 수 있을 것으로 예상된다고 발표 ✓ 푸에르토리코 정부의 사이버 보안 프로그램은 중요한 인프라의 사이버 보안과 인터넷 보안 센터의 v7 제어를 개선하기 위해 국립 표준 기술 연구소(NIST)의 프레임워크를 채택 ✓ 또한, 투명성을 높이고 구현된 모든 프로젝트와 개발 단계에 있는 프로젝트에 대해 시민들에게 알리기 위해 PRITS에서 개발한 디지털화, 혁신 관련 노력을 자세히 설명하는 2022 연례 보고서를 발표

이 슈	주 요 내 용 및 시 사 점
[중남미] 사진 편집 앱 이용으로 인한 데이터 보안 위험성 조사	▸ **Infobae(스페인어 최대 신문사), 사진 편집 앱의 데이터 보안 위험성 조사** ✓ 사진 편집 응용 프로그램, 특히 인공 지능과 연결된 기능을 제공하는 응용 프로그램의 이용이 증가하고 있으며 동 앱은 사진 갤러리 또는 스마트 폰 카메라 접근 권한을 요청 ✓ 앱 이용을 위해 일부 접근 권한은 필요하나 용도 외 과도한 데이터 접근 요청 및 다른 목적으로 데이터 이용 발생 ✓ Infobae는 과도하게 접근된 데이터가 사이버 보안 위험으로 이어질 수 있는지 확인하기 위해 9개 무작위 앱의 공유되는 데이터 유형과 용도 분석 * 9개 앱 : “Voi – AI Avatar App by Wonder”, “Laika – Editor de fotos con IA”, “ToonArt Fotos en Caricatura”, “Lensa: Editor de fotos”, “Wonder – Arte IA”, “Anime Style Foto Efecto”, “ToonMe caricaturas de ti mismo”, “Editor Voilà AI Artist”, “Mejorador de Fotos con IA” ✓ Infobae가 분석한 관련 앱들은 위치, 식별정보(메일, 이름 또는 ID), 구매 내역, 사진 및 비디오, 응용 프로그램 내 상호 작용 또는 검색 내용, 응용 프로그램 성능 및 기타 식별 데이터 (장치 유형, 카메라 데이터) 등을 수집 ✓ 앱이 수집 한 정보는 각각의 데이터 사용 및 개인 정보 보호 정책에 따라 Play 스토어 페이지 하단에서 접근 가능 ✓ 일부 경우(ToonMe 앱) 서비스를 개선하고, 제품 및 서비스 개발을 돕기 위해 데이터 접근 ✓ 대다수의 앱은 관련 데이터를 암호화하여 전송하였으며 개발자가 수집하거나 저장한 정보에 대한 삭제 요청이 가능 ✓ 그러나 "Wonder - AI Art"의 경우는 수집하는 데이터의 종류가 다양했으며 수집된 데이터가 암호화되지 않은 채 타사와 공유됨. 또한, 시스템에 업로드 된 사진의 상업화된 이용을 제한할 수 있는 방법이 없었음 ✓ 앱 개발자인 Codeway는 개인정보의 기밀성, 무결성 및 보안을 보장하기 위한 앱 정책을 확인해야 하며 바이러스 백신, VPN, 서버 내 암호화된 저장공간이 있더라도 수집된 이미지 및 비디오는 사이버 공격의 대상이 될 수 있음을 경고 ✓ 또한, 사이버 보안 전문가인 Domenic Molinaro에 따르면 시설을 보호하기 위해 널리 이용되고 있는 얼굴인식 정보와 같은 바이오 정보의 경우, 해킹하기 어렵고 암호처럼 해독될 수 없지만, 바이오 정보가 손상될 수 있음을 경고 ✓ 도난이나 분실로 인해 바이오 정보가 손상될 시, 이용자에게 지속적 위험을 미칠 수 있음 ✓ 이에, 바이오 정보 사용으로 인한 피해를 최소화하기 위해 동 정보를 이용하는 경우, 2단계 인증 프로세스를 구성하고 최신 소프트웨어 및 바이러스 백신을 확인할 것을 권장
[코스타리카] 해킹으로 인한 관광산업에 미칠 위험성 경고 및 관련 보안 방안 마련 필요	▸ **’23년, 코스타리카의 가장 큰 수입을 차지하는 관광 산업의 사이버 보안 방안 마련 필요** ✓ 사이버 범죄 전문가는 컴퓨터 시스템 오류로 인해 항공편을 놓치거나 지연될 가능성이 코스타리카 항공 및 관광산업에 위험이 될 수 있음을 경고 ✓ ’22년 코스타리카 내 CCSS(사회보장 기금)과 재무부가 사이버 범죄의 대상이 된 것과 같이, 코스타리카의 가장 큰 수입을 차지하는 관광산업이 잠재적인 해킹의 대상이 될 수 있음

이 슈	주 요 내 용 및 시 사 점
	✓ 특히 해커에 대응하기 위해 할당된 적은 예산(지출 계획의 1% 미만)은 관광 사업을 보호하기에 부족 ✓ 코스타리카 공항 이용객에 관련된 컴퓨터 운영의 보안 및 포괄적인 보안 서비스 강화 필요 ✓ Eulen Costa Rica Group의 상업 책임자인 Fernando Gamboa는 "Juan Santamaría 공항과 Daniel Oduber 공항에서 항공기 운항에 영향을 주는 공격 사례가 아직 발생하지 않았으나 '봇'에 의한 대규모 요청 발생에 따른 서버 포화 공격 등이 컴퓨터 시스템 및 웹 사이트에 영향을 줄 수 있음을 언급 ✓ 이에, 관련 전문가는 다양한 전문 기술을 통해 위와 같은 진입 및 민감한 시스템을 위반하려는 일상적인 시도가 감지되었음을 경고하며 취약성 테스트, 가능한 시나리오를 테스트하기 위한 '윤리적 해킹', 지속적인 암호 변경, 액세스 제한 및 이러한 문제에 대한 공항 내 직원의 인식제고 교육이 필요함을 강조 ✓ '23년, 더 많은 공격 시도가 예상되는 만큼 중요한 인프라, 운영 및 승객을 보호를 위한 데이터를 수집·접근할 수 있는 정부 당국, 항공사 자체 간의 조정 및 협력이 필요 ✓ 前 과기부 장관인 루이스 아드리안 살라자르는 "사이버 범죄자들이 국제 공항을 침범하여 모든 항공 운영을 무력화시킨다면 어떨까요? 국가는 이러한 유형의 폭력을 막을 준비가되어 있습니까?" 라며 대응력 제고 필요성 강조
[멕시코] 90% 공공기관이 사이버 공격으로부터 보호 능력 부족	▸ **SILIKN, 멕시코 당국에 사이버 보안 관련 강력한 법률 및 지원을 촉구** ✓ SILIKN(IT 컨설팅 회사)의 설립자인 Victor Ruiz는 멕시코 내 90% 공공·정부 기관의 90%가 사이버 공격으로부터 보호할 수 있는 능력이 부족함을 언급 ✓ 정부 기관의 사이버 취약성 분석을 수행 결과, 기관의 약 10.2%만 사고 대응 계획을 갖추고 있음 ✓ 정보기술(IT) 분야를 담당하는 인력의 78.3%가 사이버 보안 문제가 국가 안보에 위협이 된다는 것을 강조 ✓ Ruiz는 "사이버 공격의 사례 및 정교함 모두 증가하고 있으며 매주 기업과 멕시코 정부 기관에 영향을 미치는 심각한 사건이 증가하고 있다"라고 비난 ✓ SILIKN은 최근 발생한 인프라 통신 교통 사무국(SICT)의 데이터 유출 및 국방 정보 유출과 같은 사건이 연간 524,800백만 페소 이상 경제적 피해를 초래한다고 덧붙임 ✓ 또한, SILIKN은 안드레스 마누엘 로페즈 오브라도 대통령 정부기간 동안 사이버 범죄의 쉬운 표적이 되어왔음을 언급하며 멕시코 내, 사이버 보안 모범 사례가 부족하고 사고 예방과 대응을 위한 계획을 수립하려는 지도자들의 의지가 부족함을 비난 ✓ 또한 "사이버 위협, 사이버 공격자, 기술, 방법론 및 도구 문제에 대한 더 다양한 지식과 법을 구현하고 사이버 공격이 발생하는 속도 수준에 도달하는 속도가 더 빨라야 한다"고 경고 ✓ Ruiz는 컴퓨터 및 사이버 보안 서비스 관련 33억 페소 예산을 삭감한 정부에 관심을 촉구하며 예산 삭감으로 인한 업데이트, 보안 패치, 바이러스 백신 및 불법 복제 프로그램 등이 적절히 이뤄지지 않음에 따라, 수백만 명의 시민의 개인정보 유출 위험성을 경고

이 슈	주 요 내 용 및 시 사 점
[페루] 지속적인 피싱 발생에 따라 이용자의 유의사항 필요	▸ **페루, 2023년 첫째 주에 3건의 피싱 사례가 감지** ✓ '22년 1월 첫째 주, 페루 경찰 정보국은 두 개의 유명한 금융 기관에 대한 세 번의 피싱 공격을 보고 ✓ ESAN 대학의 정보기술 및 시스템 공학 교수인 Frano Capeta는 '피싱'을 사이버 범죄의 가장 일반적인 공격 중 하나이며 이용자를 위험에 빠트리는 대표적인 예로 언급 ✓ 피싱은 데이터를 훔치기 위해 신뢰할 수 있는 단체로 가장하여 이메일 또는 문자를 보내는 것으로 진행됨. 최근 Netflix 계정 혹은 은행 계좌를 사칭하여 피해 사례가 발생 ✓ 사이버 범죄 전문 검찰청에 따르면 '22년 리마 시내에서만 9,500명 이상의 사이버 공격 피해자가 있었으며 그 중 피싱이 반복적으로 발생 ✓ Indecopi 국가 소비자 보호 당국 이사회는 동 문제와 관련하여 2020년 이후 210건의 보고서가 발표되었으며 금융 기관의 주의 및 관행에 대한 변화가 필요함을 언급 ✓ Caja Piura의 사이버 보안 책임자인 Milton Villanueva는 피싱 피해를 최소화하기 위해 입금할 계좌 번호, 수령인의 이름, 금액 및 보안 페이지를 잘 살필 것을 권장 ✓ 특히 금융 거래 시, 공용 네트워크 및 WIFI를 사용하지 말고, 본인의 기기 외 장비 이용을 지양하며 사용하는 은행이나 금융 기관의 웹 사이트가 확실한지 확인이 중요하다고 강조 ✓ 또한 계좌 번호, 은행 간 코드 또는 휴대폰 번호 입력 시, 주의하며 웹사이트 주소 입력 시, 검색 창에 자물쇠가 있는지 확인 필요. 또한, 팝업창 클릭을 지양하고 개인정보나 은행 계좌를 요청하는 이메일을 신뢰하지 말 것을 권고
[코스타리카] 공공 사업 교통부 해킹 공격 발생	▸ **코스타리카, 공공 사업 교통부(MOPT) 17일 랜섬웨어 공격** ✓ 17일 화요일 코스타리카 공공 사업 교통부(MOPT)는 12개의 서버가 랜섬웨어 공격으로 암호화되었다는 성명서 발표 ✓ 국가 안보국과 과학혁신기술통신부(MICITT)의 사이버 보안 전문가가 상황을 해결하기 위해 호출되었으며 MOPT의 모든 컴퓨터 시스템이 오프라인으로 변경 ✓ 18일 국제기구에서 지원을 위해 코스타리카에 방문했다는 후속 성명 발표 ✓ 운전면허 시험은 여전히 실시되고 있으나 면허 발급 서비스가 잠시 중단되었으며 현재 재개 ✓ "가상으로 제공되었던 교통 공학 및 공공 사업, 항법 및 해상 안전 서비스는 추후 공지하여 대면으로 진행 예정"이라고 공지 ✓ MOPT는 추가 피해를 방지하기 위해 시민들에게 서비스 처리를 위해 이메일이나 전화로 정부에게 연락하지 않는다며 조심할 것을 경고 ✓ 다른 여러 기관은 추가 공격을 피하고자 MOPT와의 연결을 끊거나 연결된 서비스를 제한 ✓ 법원 시스템은 수요일 트위터에서 "링크가 다시 활성화될 때까지 교통과 관련된 벌금, 티켓 및 기타 파일을 다운로드 할 수 없다"고 발표 ✓ 도로 안전위원회는 목요일에 컴퓨터 인프라가 MOPT와 분리되어 있으며 랜섬웨어 공격의 영향을 받지 않는다고 쓴 자체 메시지를 게시했습니다. ✓ 한편, '22.5월 랜섬웨어 공격으로 차베스 대통령은 국가 비상사태를 선포한바 있음. 이는 국가 지도자가 군사 공격이나 자연재해에 대응하는 것과 동일한 방식으로 사이버 공격에 대응한 최초의 비상사태 선포 사례

이 슈	주 요 내 용 및 시 사 점
	* 코스타리카 정부는 당시 콘티가 요구한 1,000만 달러의 몸값 지불을 거부하고 여러 사이버 보안 회사와 미국, 스페인, 이스라엘 정부의 도움을 받음 ✓ 이번 공격은 아직 랜섬웨어 공격 배후가 공식적으로 알려진 바 없음
[과테말라] 사법부, 전자문서 및 서명 도입	▸ **과테말라 사법부, 전자문서 및 서명 도입 등을 위한 사이버 보안 강화** ✓ 과테말라 대법원(CSJ)은 증가하는 사이버 공격을 대응하기 위해 사법 부문의 현대화를 위한 전략 고안 ✓ IT 부문 관리를 위해 정보 및 통신 센터(CIT)와 정보, 개발 및 사법 통계 센터(CIDEJ)를 통합하여 사이버 보안을 위한 제도 마련 ✓ 또한 2023년 전자 사법 파일을 도입하고 및 모든 사법 분야 전자문서 도입 ✓ 사법부 장관 Silvia Valdés 판사는 사법부의 가상업무를 준비해 왔으며 전자문서 보관 및 변호사와 공증인을 위한 전자 서명을 도입했음을 발표 ✓ 특히, 공공기관이 표적이 된 코스타리카나 엘살바도르와 같은 다른 국가의 경험을 바탕으로 국가 기관이 사이버 공격의 희생이 되지 않도록 사이버 보안 대응력을 강화 필요성을 강조 ✓ 기관의 사이버 보안 및 전자문서 제도를 보장할 수 있도록 엔지니어 Enrique Oregel을 IT 관리자로 임명 ✓ 동 관리는 1.컴퓨터 보안, 2.행정 컴퓨터 시스템, 3.컴퓨터 및 행정 서비스, 4서비스 운영 등 네 가지 영역으로 구성
	▶ **시사점** ✓ 중남미 지역 내 정부는 금년 사이버 공격이 증가할 것으로 예측하며 대응 강화를 위한 정책 등을 발표 ✓ 특히, 코스타리카는 작년 5월 Conti 랜섬웨어의 광범위한 공격으로 여러 부처가 마비된 지 불과 몇 달 만에 또 다른 랜섬웨어 공격을 받아 정부부처 홈페이지 서비스가 중단됨 ✓ 중남미 지역 내 국가 단위의 정보보호 사업 추진 정보 동향을 살피고 한국 기업 진출 및 수주를 위한 관심 필요

KISA 정보보호 해외진출 전략거점(중동) 1월 주요동향

2023. 1. 31(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[중동] 중동 사이버범죄 주요 표적	▸ **GCC 사이버범죄의 주요표적은 사우디아라비아와 UAE** ✓ 사이버 보안 회사인 Group-IB가 발표한 보고서에 따르면 2021년 중반에서 2022년 중반 사이에 GCC(Gulf Cooperation Council) 국가 중 사우디아라비아와 아랍에미리트의 조직이 사이버 공격의 가장 큰 표적이 되었다고 함 ✓ 연구에 따르면 랜섬웨어 운영은 중동과 북아프리카 지역을 포함한 전 세계 기업과 조직에 가장 심각한 사이버 위협이 되고 있음 ✓ 랜섬웨어는 파일을 암호화하여 대상 조직이나 개인이 장치 및 장치에 저장된 데이터에 액세스하지 못하도록 하는 악성소프트웨어 유형으로 대부분의 경우 범죄 집단은 복호화 대가로 몸값을 요구하며, 몸값을 지불하지 않으면 훔친 데이터가 공개되거나 삭제될 수 있음 ✓ 연구 결과에 따르면 2021년 하반기부터 2022년 상반기 사이에 GCC에서 42건의 랜섬웨어 공격이 있었으며 UAE와 사우디내의 조직이 대부분이었고 대상의 33%는 UAE에, 29%는 사우디가 차지 ✓ 이 보고서는 또한 에너지, 통신, IT 및 제조 부문이 사이버 갱단의 가장 큰 표적이 되고 있다고 함
[바레인] 바레인 정부 사이버보안 훈련	▸ **바레인 TRA, 사이버 보안 훈련 실시** ✓ 바레인의 통신규제청(TRA, Telecommunications Regulatory Authority of Bahrain)은 사이버위협에 대한 문제를 찾고 해결하기 위한 사이버 보안 훈련 추진 ✓ Cyber Ranges사와 협력하여 진행한 훈련은 운영자가 사이버 위협을 처리하는 능력을 테스트할 수 있도록 보안 훈련을 실시 ✓ 또한 조직이 현재 및 향후 위협에 대처할 준비가 된 유능한 사이버 보안 인력을 양성할 수 있도록 기회를 제공 ✓ 이 훈련은 조직 내에서 사이버보안 절차에 대한 연습을 진행하고 이에 대한 대비를 강화하여 기술과 지식을 향상시킴 ✓ TRA는 통신 부문의 사이버 훈련은 사이버 보안 문제가 효과적으로 해결되도록 보장할 것이며, 적절한 비상 계획에 대한 요구 사항을 설정한다는 점에서 매우 중요하게 생각한다고 함
[사우디] 사우디 디지털 보안 인력	▸ **사우디아라비아 디지털 보안 분야 채용 확대 필요** ✓ LinkedIn의 연구에 따르면 디지털 보안은 사우디아라비아에서 지속 가능성, 판매 및 기술과 함께 가장 빠르게 성장하는 직업 분야 중 하나 ✓ 보안 운영 센터 분석가와 사이버 보안 관리자는 모두 이 지역에서 가장 수요가 많은 직업 중 상위 10위를 차지하고 있으며 전통적인 보안 요원에 대한 수요도 지속적으로 증가 ✓ LinkedIn에 따르면 기술 변화와 역할의 증가에 따라서 해당영역의 확대와 증가가 지속적으로 이루어 지고 있고 사우디아라비아의 상위 10개 역할 중 4개는 사이버 보안, 데이터 분석 및 소프트웨어 개발 분야라고 함

이 슈	주 요 내 용 및 시 사 점
	▸ **시사점** ✓ 중동의 2022년 사이버 범죄의 주요 표적은 사우디아라비아와 UAE로 석유 에너지 시설이나 통신시설 등에 많은 공격이 있었음 ✓ 사우디아라비아는 사이버범죄의 증가와 이에 따른 사이버 보안 수요로 인해 관련 전문 인력의 확대가 필요한 상황 ✓ 바레인은 사이버위협에 대한 대비를 위해 보안 훈련을 실시