KISA 정보보호 해외진출 전략거점(동남아) 2월 주요동향

2023. 02. 28(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
싱가포르-말레이시아 협력 강화	▸ **싱가포르와 말레이시아는 디지털 경제에 대한 양자 협력 강화 약속** ✓ 양국은 2월 3일 개인 정보보호, 사이버 보안 및 디지털 경제에 대한 양자 협력 강화에 대한 약속을 재확인 ✓ 쿠알라룸푸르에서 열린 제 6차 정보통신협력 공동위원회에 참석한 말레이시아 통신 및 디지털부 사무총장 Datuk Seri Mohammad mentek와 싱가포르의 Joseph leong 통신 및 정보 사무차관과 성명서 발표
인도네시아 정부/교육기관 차단	▸ **인도네시아 통신정보부는 683개의 정부 및 교육 사이트를 차단** ✓ 통신정보부는 온라인 도박 콘텐츠로 인해 손상된 정부 사이트 461개 도메인과 222개의 교육 사이트 도메인을 차단하였다고 발표 ✓ 교육부는 통신 및 정보학 장관규정에 의해 감시 상태인 도메인을 일시적으로 非활성화 할 권한이 있음
2022년 동남아 5대 사이버 침해사고 발표	▸ **2022년 동남아 5대 사이버 침해사고를 발표** ✓ 말레이시아 Maybank, Astro 및 EC의 1,300만 고객정보 유출 사고를 1위로 선정. 말레이시아 Cybersecurity Malaysia(CSM)과 Department of Personal Protection(JPDP)가 수사 중 ✓ 2위는 AirAsia Group을 상대로 5백만명의 고객정부가 유출된 사건이 선정. 이 사건으로 고객의 이름, 생년월일, 국적, 출장지 등의 개인정보가 유출되었음 ✓ 3위는 말레이시아 National Registration Department 데이터 유출 사고가 선정. 본 사건으로 1940년에서 2004년에 출생한 2,250만명의 말레이시아 성인의 개인정보가 유출되었음 ✓ 4위 필리핀의 선거관리위원회의 보안시스템이 해커그룹에 의해 침해되어 60TB의 개인 유권자 정보가 노출된 사고가 선정 ✓ 5위는 Bjorka라는 해커에 의해 13억개의 인도네시아 SIM 카드 등록 프로필이 유출된 사고가 선정. Bjorka는 인도네시아 대통령과 국가정보원간의 통신 로그를 노출시킨바 있으며 유명 정치인의 연락처와 예방 접종 번호를 공개한 바 있음 ✓ 최근 Surfshark의 통계에 따르면 말레이시아, 일본과 한국의 데이터 유출 사고가 각각 -77%, -81%, -77% 감소하였으나 베트남은 436%, 필리핀 238%, 인도네시아는 1368% 증가하였음

KISA 정보보호 해외진출 전략거점(북미) 2월 주요동향

2023. 02. 28(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[미국] 5년 만에 처음이자 사상 최대 규모의 NIST 사이버보안 프레임워크(CSF)의 변화 계획	▸ **NIST, 사이버보안 프레임워크(CSF) 사상 최대 규모 개혁 계획** ✓ 2014년에 처음 게시된 2018년에 버전 1.1로 업데이트된 CSF는 사이버 보안 위험 관리를 위한 일련의 지침과 모범 사례 프레임 제공 ✓ 이 프레임워크는 규범적이기보다는 유연하고 적응 가능하도록 설계 되었으며 미국 내외의 조직 및 정부 기관에서 사이버 보안 프로그램을 만들고 성숙도를 측정하는 데 널리 이용 ✓ NIST는 오랜 협의 끝에 CSF 2.0에 대한 개념 문서를 발표하고 추가 검토를 위해 공개했음 ✓ 피드백은 수정된 프레임워크의 최종 초안을 개발하는 데 사용되며 올 여름에 나올 예정임 ✓ NIST의 수석 기술 정책 고문이자 사이버 보안 프레임워크 프로그램 책임자인 Cherilyn Pascoe는 “이번에는 중요한 업데이트를 보장할 만큼 사이버보안 환경에 충분한 변화가 있었다고 생각함”이라고 말함 ✓ “NIST뿐만 아니라 다른 곳에서도 사이버 보안 표준에 변화가 있었고, 위험 환경과 기술에 상당한 변화가 있었음 ✓ 응답자 대다수가 여전히 프레임워크가 마음에 든다고 말했지만 사람들이 찾고 있는 변경 사항이 많았기 때문에 우리가 새로 고칠 때라고 생각함” ✓ 주목할 만한 변화 중 하나는 프레임워크의 대상이 누구인지이고, CSF 1.1이 발행된 이후 미 의회는 NIST가 원래 목표로 삼았던 주요 국가 인프라 조직(공익사업, 통신, 운송, 은행 등)을 넘어 소기업 및 고등교육기관의 요구 사항을 고려하도록 NIST에 명시적으로 지시함 ✓ Pascoe는 “이 범위는 원래 미국 대통령 행정 명령에 따라 정의 된 중요 인프라를 위한 것이었지만 시간이 지남에 따라 많은 조직에서 사용하기 시작했음” 이라고 말함 ✓ “우리는 조직이 중요한 인프라인지 여부를 결정해야 하는 것을 원하지 않았고, 이는 때때로 추가 부담을 수반하는 법적 문제이며, 그래서 모든 조직으로 확대할 것을 제안” ✓ 또한 국제 협력을 강화하고 더 많은 국가가 전체 또는 부분적으로 프레임 워크를 채택하도록 장려할 계획임 ✓ 새로운 ‘거버넌스’ 기능은 금융 안정성에 대한 위협과 같은 다른 기업 위험과 함께 사이버보안 위험을 포지셔닝하기 위해 기존의 5가지 원칙(식별, 보호, 감지, 대응 및 복구)에 합류 ✓ 새로운 기능에는 조직, 고객 및 더 큰 사회의 우선순위 및 위험 허용 범위 결정이 포함 되며, 사이버 보안 위험 및 영향 평가 사이버 보안 정책 및 절차 수립 사이버 보안 역할 및 책임에 대한 평가 ✓ “사이버 보안 위험이 재정적 위험과 함께 다른 기업 위험이 일부로 통합될 수 있는 방법을 더 잘 이해하기 위한 많은 직업이 있음. 사이버 보안 위험과 사이버

이 슈	주 요 내 용 및 시 사 점
	보안을 해결하기 위해 시행해야하는 정책 및 절차를 인식하는 고위 경영진의 중요성"이라고 Pascoe는 주장함 ✓ "사이버 보안이 단지 기술적인 문제가 아니라 조직의 상위 수준에서 해결해야 하는 문제라는 인식이 훨씬 더 높아졌다고 생각 함" ✓ 이러한 추가는 주로 기술 전문가와 고위 관리자 간의 사이버 보안 위험에 대한 논의를 구조화하기 위해 프레임워크 사용이 증가함에 대한 대응임 ✓ (위기관리) 처음으로 새로운 프레임워크는 공급망 위험 관리에 중점을 두고 조직이 클라우드 컴퓨팅에서 컴퓨터, 소프트웨어 및 네트워킹 장비에 이르기까지 모든 종류의 제3자 위험과 비기술적 위험을 해결하도록 돕고 장려 ✓ Pascoe는 이를 수행하는 방법에 대해 엇갈린 의견이 있다고 말했고, 특히 사이버 보안 공급망 관리를 프레임워크의 기존 구조에 통합해야 하는지 아니면 별도의 기능으로 분리해야 하는지에 대해 설명함 ✓ "이것은 정말 중요한 문제이고 생각하지만 피드백은 엇갈림. 그래서 우리는 이것과 해결 방법에 대해 좀 더 생각하자고 말했음" ✓ "때로는 부문별로 진행되며 때로는 기존 규제 요구 사항을 기반을 함. 예를 들어 금융 부문은 사이버 보안에 대해 규제가 심하고 프레임워크 내에서 보고자 하는 기존 제3자 요구 사항이 있으므로 아마 제3자에 대한 상단한 확장을 원하는 것에 대해 가장 목소리를 높일 것임" ✓ 측정을 위한 측정 CSF 2.0은 또한 기본 위험 관리 프로세스에 관계없이 조직의 측정 및 평가 노력의 결과를 전달하기 위한 공통 분류법 및 어휘와 함께 측정 및 평가에 대한 더 많은 지침을 포함하도록 설정됨 ✓ "NIST는 측정 과학 기관이므로 우리는 항상 사물을 측정하는 도구를 개발하기 위해 노력하고 있음. 하지만 사이버 보안 측정은 아마도 우리가 지금까지 다루어 본 것 중 가장 어려운 것 중 하나임" ✓ (프라이버시, 제로 트러스트 수수께끼) NIST는 이해 관계자와 협의한 후 프라이버시 프레임워크를 CSF와 병합하지 않기로 결정했지만, Pascoe는 "돌 사이 중복"이 증가함에 따라 향후 CSF 3.0을 위한 움직임이 될 수 있다고 말함 ✓ Pascoe는 제로 트러스트 프레임워크 내에서의 프레임워크 내에서의 적용 가능성과 같은 주제에 대한 의견 불일치 또는 적어도 상당한 추가 논의를 예상. 제로 트러스트는 조직이 조직의 경계 외부에 있든 내부에 있든 관계없이 기본적으로 어떤 장치도 신뢰하지 않도록 촉구하는 네트워크 보안 개념 ✓ NIST는 제로 트러스트를 프레임워크에 통합할 필요가 없다는 입장이며, 아키텍처를 적용하는 것이 바이든 행정부의 우선순위임
[미국] 사이버 보안이 개선됨에 따라 한 해커 그룹이 45명의 직원을 해고함	▸ **해커들도 범죄 조직에 의해 해고되었음** ✓ 랜섬웨어 위협을 영속시키는 해커와 다른 사람들은 불안정한 고용 시장을 탐색하는 최신 기술 산업 근로자임 ✓ 월스트리트 저널 보고서에 따르면 미국 법무부 조사관과 기업이 사이버 보안 위협에 대한 감독을 강화함에 따라 랜섬웨어 공격의 영향이 둔화됨 ✓ 사이버 보안 그룹은 WSJ에 경계 강화로 인해 특정 사이버 보안 전문가가 작년에 수행한 온라인 램섬웨어 공격의 수와 해커가 이를 위해 시도한 몸값 지불 규모가 모두 감소했다고 말했음 ✓ 콘티(Conti)라는 한 해커 그룹은 지난해 콜 센터가 돈을 벌지 못한 후 랜섬웨어

이 슈	주 요 내 용 및 시 사 점
	공격을 퍼뜨리기 위한 명백한 계획의 일환으로 일하고 있던 콜센터 운영자 45명을 해고하기도 했다고 이 매체는 정보기관인 레드 센트(Red Sense)의 임원을 인용해 보도함 ✓ 랜섬웨어 해킹은 특히 해커가 지불금을 추출하기 위해 개인 정보를 대상으로 협박할 때 큰 위험을 초래할 수 있음 ✓ DOJ는 최근 몇 년 동안 사이버 범죄에 대한 단속을 강화하고 있다는 신호를 보냈음. 2021년에 기관 National Cruptocurrency Enforcement Team과 Ransomware and Digital Extortion Task Force를 포함하여 내부적으로 새로운 그룹을 만듦 ✓ 이러한 노력은 법무부가 해커 혐의를 조사하고 미국 송화하는 데 도움이 되었다고 이 기관은 말했고, 예를 들어, 연방 검사는 작년에 폴란드에 구금된 한 남자를 연방 법원에 출두시켰음 ✓ 에이전시는 그가 소프트웨어 포함한 회사를 대상으로 Sodinokibi/REvil 랜섬웨어를 사용했음 ✓ 이 기관은 또한 2021년 미국 동부 해안에 서비스를 제공하는 5,000마일의 가스 파이프라인에 영향을 준 콜로니얼 파이프라인 해킹을 포함하여 국내 인프라에 대한 세간의 이목을 끄는 공격 속에서 감독을 강화했음 ✓ 법무부는 지난 7월 사이버 보안 보고서에서 “100개 이상의 랜섬웨어 변종”을 조사하고 있으며 “피해자에게 10억 달러 이상의 손실을 입힌 것으로 의심되는” 그룹을 분류했음 ✓ 연구 및 컨설팅 회사인 Gartner에 따르면 국가는 일반적으로 랜섬웨어 공격에 대한 감독을 강화하고 개인 정보 보호 규정을 개선하려고 노력하고 있음 ✓ 회사는 내년에 예상되는 사이버 보안 동향에 대한 6월 보고서에서 2025년까지 국가의 거의 1/3이 랜섬웨어를 관리하는 법률을 제정할 것으로 예상함 ✓ 2021년에는 그 수치가 1% 미만이었음
	▸ **시사점** ✓ NIST에서 사이버 보안 위협 대응을 위한 거버넌스의 개선 작업으로 보안 프레임 워크를 새롭게 변화했음 ✓ 이러한 보안 프레임 워크의 변화와 함께 국제 사회와의 소통을 강조했으며, 대한민국도 이를 받아들이고 보안 프레임 워크의 상황에 맞게 적을 할 필요가 있음 ✓ 해커들은 최근 범죄 조직에서의 보안 대응의 강화로 해커 조직으로부터 해고되는 과정을 겪었음. ✓ 랜섬웨어의 대응력 강화는 대한민국 역시도 강조했던 부분이고, 해커들의 영향력 약화를 가져 왔음

KISA 정보보호 해외진출 전략거점(아프리카) 2월 주요동향

2023. 02. 28(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[나이지리아] 주요 사이버 범죄 조직망 강화 발표	▸ **사이버 위협 협력 증가와 함께 사이버취약점 촉발 경고** ✓ 사이버위협에 대한 협력 증가 및 저비용 악성코드 확산 등에 대한 경고(HP) * 경기 침체와 불확실성 증가에 따른 사이버범죄 심화 예상('23) ✓ 조직적 사이버위협에 대한 예방책 권고 발표(나이지리아 보안 담당) * 사이버범죄 관련 예산 강화, 운영체제 아래의 공격적 투자, 원격 장비 공격 대비 등
[케냐] 출생 및 사망 관련 전자문서 관리 개시	▸ **케냐 디지털 출생 및 사망 증명서 발급 개시** ✓ 디지털 출생 및 사망 증명서 발급에 따라 고유식별 분류(UPI) 시스템 활용 가능 * UPI(Unique Personal Identifier) : 18세 도달 시 ID번호 및 운전면허증 번호 역할 ✓ 고유 식별 등 전자문서화는 입학 및 국가시험 등 다방면 활용 예정 ✓ 본 정부서비스의 향상은 전체 정부서비스의 디지털화 목표와 일치
[세이셸] 경찰청 내 사이버 범죄 수사대 구성 및 국제공조 강화	▸ **사이버범죄 대응을 위한 전담 기구 설치 및 국제 협력 강화** ✓ 세이셸 사이버범죄 수사대 설치를 위한 경찰청-인터폴 논의 개시 * 온라인 사기 등 증가하는 사이버 범죄 대응을 위한 조직 필요성 증대('22) ✓ 인터폴은 세이셸 내 여성 및 어린이 대상 사이버범죄 예방 관련 캠페인 시행 추진 中 ✓ 사이버범죄 예방 관련 시스템 및 DB 액세스 강화 등 국제 협력을 통한 범죄 예방 강화
[르완다] 모바일 대상 사이버범죄 증가에 대한 인식제고 필요	▸ **국가 정책(Connect Rwanda)에 따른 사이버범죄 가능성 대두** ✓ 르완다 내 기하급수적 휴대전화 보급률(전국민 83% 이상) 등 뚜렷한 성장세 * 금융 포용 심화 정책 등으로 교육지원 및 정보 공유의 사회적 기능 강화를 위해 스마트폰 보급률(20% 미만) 상승 이니셔티브 진행 中 ✓ 이러한 정책은 사이버 범죄 가능성 상승 예상되며 예방 조치 강화 필요 ✓ 사이버 범죄에 대한 대중 교육과 함께, 피해 예방을 위한 선제적 조치 권고
	▸ **시사점** ✓ 아프리카 국가는 타 국가와 마찬가지로 전자정부 도입 및 시스템 구축 등에 노력 中이나, 사이버보안 대비를 위한 예산 투입 등의 노력은 현저히 부족 ✓ 사이버범죄 증가에 따라 개인정보 피해 등이 발생 예상되며, 향후 이러한 대응 마련이 필연적으로 증가할 것임

KISA 정보보호 해외진출 전략거점(중남미) 2월 주요동향

2023. 02. 28(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[코스타리카] MICITT (과기부) 장관 사퇴	▸ **코스타리카, MICITT(과기부)를 포함한 3개 부처의 장관 사임** ✓ 공화국 대통령 로드리고 차베스 로블레스 (Rodrigo Chaves Robles)는 기자회견에서 세 부처의 지도자 변경을 확인 ✓ 차베스 대통령은 2월1일 MICITT 과학혁신기술통신부 장관 '카를로스 엔리케 알바라도 브리세뇨'와 코스타리카 수로 및 하수도 연구소(AyA)의 대표 '로베르토 구즈만 구티에레즈', 농촌 개발 연구소(INDER)의 대표 '에두아르도 로버트 우레냐'의 사임을 알림 ✓ 공공사업 교통부 인프라 차관을 역임 한 알레한드로 길렌 과르디아가 AyA 대표직을 맡을 것이며 오스발도 아르타비아 카르발로가 INDER 대표직에 임명, 현재 대외 무역 차관인 폴라 보간테스 사모라(Paula Bogantes Zamora)가 새로운 과학, 혁신, 기술 및 통신 장관(MICITT)으로 임명 * MICITT에 새로 부임한 Paula 장관은 국제 무역 부문 석사 학위, 경영 학사 학위 및 조직 리더십 대학원 학위를 보유하고 있으며 사이버보안, AI 및 블록체인에 대한 경험을 갖춤 ✓ 또한 작년 9월부터 공석으로 남아 있던 사회보장청(CCSS)의 장관은 '안드레스 로메로 로드리게스'가 새로운 임명 ✓ 대통령에 따르면 INDER, AyA 및 MICITT의 새로운 지도자들은 이미 이사회에서 승인되어 즉시 역할을 시작할 예정이며, MICITT 새 장관의 경우 현재 진행 중인 국제 선교 사업에서 돌아온 후 업무 시작 예정 ✓ 차베스 대통령은 그동안 고생해준 지도자들에 감사 인사를 전하며, 인사변경의 이유로 각 분야 핵심 성과 지표에 대한 진행 속도, 관점, 달성 경과 등을 평가한 후 내린 결정이라고 발표
[스페인] 11개사 주요 사이버보안 제공업체 소개 * 중남미 지역 스페인 보안업체 영향력이 큼	▸ **Computing es(스페인 ICT 동향 미디어 회사), 11개 주요 사이버 보안 회사 강점 소개** ✓ 스페인에 위치한 ICT 동향을 제공하는 Computing es 회사에서 사이버보안 관련 탑11개 회사(국내 기업 삼성 포함) 서비스를 소개 ✓ 사이버보안 회사는 현재 정보 시스템의 무결성과 데이터의 기밀성을 보장하는 사이버보안 서비스 및 보안 솔루션을 제공하여 조직이 모든 유형의 사이버 공격으로부터 방어할 수 있도록 지원하는 데 필수적으로 필요 ✓ 사이버보안 회사를 통해 멀웨어, 피싱, 랜섬웨어, 데이터 침해, DDoS 등의 공격으로부터 보호 가능. 또한 SOC(보안 운영 센터) 또는 경우에 따라 CISO를 통해 관리형 서비스를 제공 ✓ 스페인의 사이버 보안 회사는 클라우드 서비스와 인텔리전스 기능을 제공하며 11개 회사를 추천 **① 아카마이** ✓ Akamai는 직원과 고객이 매일 사용하는 애플리케이션, API, 네트워크 액세스,

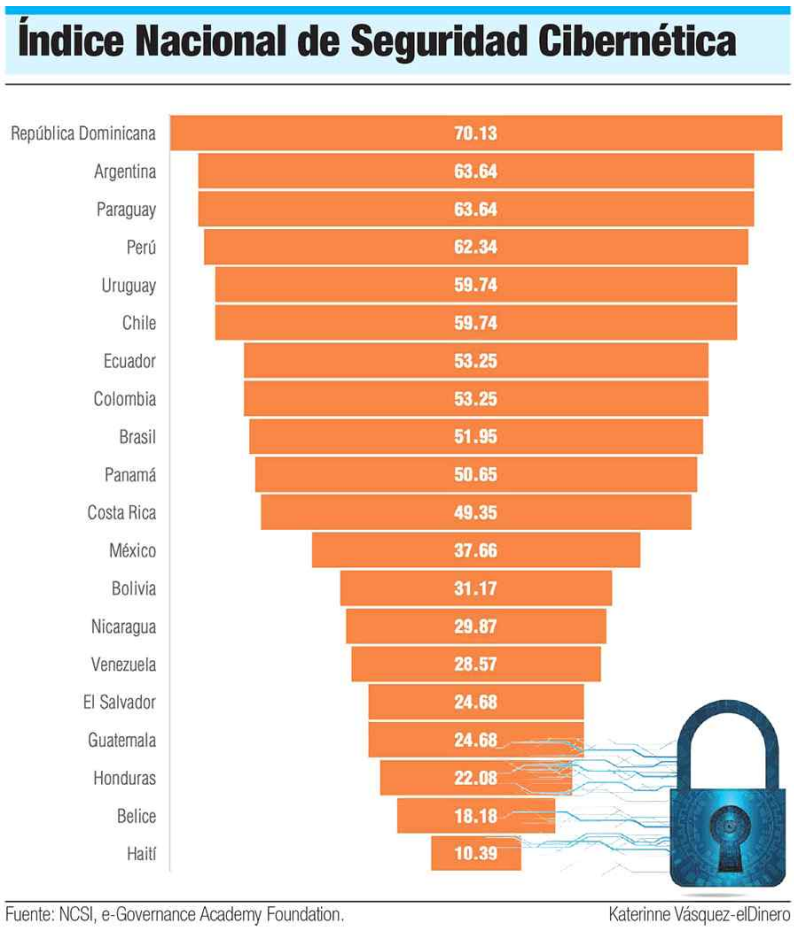
이 슈	주 요 내 용 및 시 사 점
	자격 증명 등 모든 상호작용 보호 서비스 제공 ✓ 글로벌 위협에 대한 플랫폼의 가시성을 사용하여 전략적 파트너로서 혁신, 확장 및 변환이 필요한 모든 곳에서 보안을 제공 ✓ DDoS 보호 기능 및 클라우드 상 애플리케이션, 데이터 센터 및 인프라에 사이버 공격이 도달하기 전 차단. 제로 트러스트 보안을 활성화하여 IT 환경을 완벽하게 보호 **② OneseQ (알함브라의 사이버보안)** ✓ OneseQ는 공격을 예방, 탐지 및 대응하여 기업의 보안을 보장하는 것을 목표로 하며 각 조직의 비즈니스에 맞게 조정된 혁신적인 사이버보안 솔루션을 제공 ✓ 식별, 보호, 감지, 대응, 복구 및 학습 절차를 통해 서비스를 제공하며, 침입 탐지, 고급 취약성 관리, 엔드포인트 탐지 및 대응 서비스를 가능하게 하는 자체 24×7 SOC의 경우 국가 SOC 네트워크의 일부 CERT (사고 대응 센터), TF-CSIRT 및 주요 보안 및 사이버 보안 제조업체와 적극적으로 협력 **③ GMV** ✓ 12개국에 진출한 기술 그룹과 3,000명 이상의 우수한 전문가로 구성된 팀으로 사이버보안의 세계에 거의 30년 동안 헌신해 온 그들은 기존 위협을 식별하고, 자산을 보호하고, 공격 시도를 탐지하고, 발생할 경우 가능한 한 빨리 상황을 복원 ✓ 기존 취약성을 발견하고 클라우드가 제공하는 기능을 활용하여 멀웨어를 탐지하는 방법을 보여줌 ✓ 인공 지능 이용 및 DevSecOps 철학을 적용하여 민첩하고 탄력적으로 서비스 제공. 또한 침입 탐지 및 방지 솔루션 또는 스마트 키를 사용하여 커넥티드 카의 사이버 위험을 관리 **④ Hornetsecurity** ✓ Hornetsecurity는 독일 최고의 이메일 클라우드 보안 및 엔드포인트 백업 제공업체로, 모든 규모의 기업과 조직을 위해 IT 인프라, 디지털 통신 및 데이터를 보호 ✓ 8천개 이상의 파트너와 MSP와 함께 지속적으로 성장하는 초국가적 네트워크를 보유 ✓ 이 회사는 전 세계 12개의 보안 데이터 센터를 통해 서비스를 제공 ✓ 혁신적인 기술을 통해 Hornetsecurity는 현재 규정에 따라 스팸 및 바이러스 필터링, 피싱 및 랜섬웨어 보호, 보관 및 암호화를 포함하여 이메일 보안의 모든 중요한 영역을 포괄하는 포괄적인 솔루션을 제공 **⑤ Kaspersky** ✓ Kaspersky는 200개 이상의 국가에서 4억 명 이상의 사용자와 24만명의 기업 고객을 보유한 전 세계 기업, 중요 인프라, 정부 및 소비자를 보호하기 위한 보안 솔루션 및 서비스를 개발한 25년의 경험을 가진 글로벌 사이버 보안 회사 ✓ Kaspersky의 분석 시스템은 2022년에 배포된 평균 400,000개의 악성 파일을 탐지했으며, 이는 전년 대비 5% 증가한 수치 ✓ Kaspersky는 최근 Kaspersky Standard, Kaspersky Plus 및 Kaspersky Premium으로 구분된 새롭고 단순화된 솔루션 포트폴리오를 출시했으며 각 플랫폼의 Windows, Mac, iOS 및 Android 모바일 장치에 대한 보호 기능을 제공

이 슈	주 요 내 용 및 시 사 점
	⑥ OpenText Cibersecurity ✓ OpenText Cybersecurity는 사이버 탄력성, 저항 능력의 개념을 중심으로 전략을 집중. 이를 위해 비즈니스의 기반이되는 세 가지 디지털 ID, 데이터 및 애플리케이션을 보호하고 방어하는 완전한 솔루션 제공 ✓ OpenText 사이버 보안은 사이버 복원력의 주요 측면을 다루며 예측, 저항, 복구 및 진화; 조직의 탄력성을 보장하기 위해 솔루션을 제공 ✓ 전문 분야로는 ID 관리 및 접근 거버넌스, 보안 운영, 애플리케이션 보안, 개인 정보 보호 및 데이터 거버넌스가 포함 ⑦ Samsung ✓ 삼성은 기업이 비즈니스에서 정보를 디지털화하고 보호하는 데 도움이 되는 모바일 솔루션을 개발 ✓ 한국 회사의 경우 하드웨어 및 소프트웨어의 통합 보안, 실시간 보호 및 파트너와의 열린 협업이 진행 가능한 Samsung Knox의 전체적이고 다층적인 접근 보호 방식 덕분에 신뢰를 얻음 ✓ Samsung Knox는 보안 및 관리 측면에서 회사의 요구 사항을 충족하는 일련의 클라우드 서비스를 제공하며 이 서비스에는 보안 솔루션, 정책 관리, 운영 체제 버전 제어, 터미널의 동작을 보여주는 데이터 분석 및 회사의 전체 터미널 자동 등록이 포함 ⑧ Seidor ✓ Seidor는 혁신, 고객 경험, ERP, 분석, 직원 경험, 클라우드, 직장 및 사이버 보안을 위한 포괄적인 솔루션 및 서비스 포트폴리오를 제공하는 기술 컨설팅 회사 ✓ Seidor는 유럽, 라틴 아메리카, 미국, 중동, 아프리카 및 아시아의 40개국에 직접 진출하여 8,500 명 이상의 고객에게 서비스를 제공 ✓ 컨설팅을 위해 SAP, 마이크로 소프트, IBM, 어도비 및 시스코 등과 협력하며 Seidor는 고객에게 사이버 보안 전략, 자산의 위험을 관리하고 당국에 대한 비즈니스 규정 준수 및 인증 요구에 대응할 수 있는 컨설팅을 제공 ⑨ WatchGuard ✓ 사이버보안 분야에서 25년 이상의 경험을 가진 다국적 기업인 WatchGuard는 하드웨어, 소프트웨어 및 서비스를 결합하여 네트워크 보안 솔루션에서 Wi-Fi 보안, 다단계 인증(MFA), 고급 엔드포인트 보호에 이르기까지 다양한 조직에서 견고한 방어를 구축하는 광범위한 포트폴리오를 보유 ✓ 또한, 네트워크 보안 서비스에서 맬웨어 방지 및 기밀 정보 보안을 위한 솔루션 제공. 동 제품에는 EPDR 도구, 제로 트러스트, 위협 헌팅 서비스 및 최신 SOC를 위한 솔루션도 포함 ⑩ Wise Security Global ✓ 와이즈 시큐리티 글로벌은 사이버 보안의 모든 차원에 특화된 기술 회사로, 사이버보안의 모든 차원에 대응하여 사이버 신뢰성과 보안 환경을 조성 ✓ 현재 스페인의 여러 사무실에 100명 이상의 전문 전문가가 있습니다. 서비스를 통해 NIST 프레임워크의 모든 기능을 다루고 C-SOC에서 탐지 및 응답 서비스를 제공하며 모든 유형의 조직에 사이버 보안에 대한 액세스를 제공 ✓ 동 사는 해당 부문의 규정 및 프레임워크에 부합하는 사이버보안 거버넌스 모델을 구현하고 CISOaaS(CISO as a Service) 모델을 사용하면 절차와 구현을 단순화하여 사이버보안 서비스를 아웃소싱 할 수 있음

이 슈	주 요 내 용 및 시 사 점
	⑪ Zyxel ✓ 클라우드 플랫폼 Nebula를 통해 결제 장치 및 시스템, 모바일, IoT 장치에서 안전하고 빠른 Wi-Fi 연결을 제공 ✓ 5G/LTE 라우터를 통해 '항상 연결' 가능한 서비스를 제공함으로써 인터넷 연결이 불안정한 지역의 보안을 보장 ✓ Zyxel은 무선 액세스 포인트에서 유연하고 안전한 보안 솔루션을 제공하여 직원 및 고객 액세스를 지원 **<다가오는 사이버 공격의 도전과제>** ✓ 지능형 멀웨어 : 최신 멀웨어는 더 쉽게 적응하고 서명 감지를 피하기 위해 모양 변경 가능. 공격자는 다른 방법을 사용하여 멀웨어 파일을 바이너리 수준으로 반복적으로 변경할 수 있으므로 바이러스 백신 소프트웨어에서 다르게 보일 수 있음 ✓ 랜섬웨어 : 정교한 방법을 사용하여 기존의 랜섬웨어 탐지 조치를 회피하고 일반적인 프로세스를 활용하여 시스템에 침입. 이러한 방식으로 데이터 도난 및 암호화를 찾기 위해 네트워크를 이동하며 공격 대상자에게 유출된 데이터나 인증 정보를 판매하거나 유출하겠다고 위협 ✓ 피싱 : 정교하고 발전된 사회 공학을 사용한 피싱 공격 발생. 또한 같은 방식으로 스미싱 및 모바일의 SMS를 통해 공격 진행 ✓ 재택근무 증가를 이용하여 홈 네트워크 공격을 통해 회사 시스템에 진입하는 기술 : 침입 방법으로서의 인공 지능, 이용 습관 학습, 신원 도용, 문서 위조 ✓ 딥 페이크 : 공격 대상자를 정확하게 속일 목적으로 인공 지능을 사용하여 허위 이미지, 동영상 또는 시각적 요소를 사용하여 만든 메시지로 많은 영역에 적용될 수 있음
[중남미] 도미니카 공화국, 중남미 지역 내 사이버 보안 선두주자	▸ **중남미 지역이 당면한 사이버보안 위험성 및 국가별 사이버보안 지수** ✓ 중남미 지역 당면한 가장 큰 위험성 중 하나는 관광, 은행, 금융 시스템에 이르기까지 모든 부문에서 발생하는 사이버 보안 문제. 국제 형사 경찰기구(Interpol)는 동 지역 내 사이버 범죄 공격이 증가하고 있다고 발표 ✓ 2020년 상반기에만 중남미 지역은 세계에서 가장 높은 사이버 공격률을 기록했으며, 모바일 브라우저를 통한 사고는 전 세계 평균보다 약 3배 높았음 ✓ e-거버넌스 아카데미가 개발한 국가 사이버보안 지수 (NCSI)에 따르면 도미니카 공화국은 디지털 개발 능력이 여전히 부족하지만 동 지역 내 가장 높은 사이버 보안 지수등급인 70.13 달성 ✓ 이는 캐나다(70.13)와 동률이며 미국(64.94)과 같은 다른 국가를 능가하는 전 세계 상위 30위 안에 든 점수 ✓ 사이버보안은 모든 부문에서 지속해서 관련성을 가지는 문제로 중남미 지역도 예외는 아니며 정부, 기업 및 사용자가 디지털 보안에 점점 더 관심을 가지고 있다고 ESET 라틴 아메리카의 컴퓨터 보안 전문가인 Miguel Ángel Mendoza는 설명 ✓ e-거버넌스 아카데미는 보안 지수 평가를 위해 사이버 보안 정책 개발과 같은 일련의 지침 유무를 평가했으며 도미니카 공화국, 파라과이, 칠레 및 에콰도르가 이를 갖추고 있다고 전달

이 슈	주 요 내 용 및 시 사 점

<중남미 지역 내 사이버보안 지수 순위>



✓ 또한 카리브해 지역 국가 및 우루과이가 사이버 위협의 분석 및 정보 측면에서 필요한 표준을 가진 유일한 국가로 평가됨

* 필요한 표준 : 국가 사이버 보안 관측소(Ciberobservatorio) 및 사이버보안 운영 센터 부서(SOC) 유무

✓ 평가 기준으로 사이버 보안 역량을 포함하여 해당 지역 내 교육 및 전문성 개발이었으며 이 부문에서는 아르헨티나와 파나마에만 관련 제정이 있는 것으로 평가

✓ 하지만 도미니카 공화국의 CSIRT Nacional은 사이버 범죄 협약의 일부인 FIRST의 정회원으로 2020년 인정되었으며 중남미 지역 내 사이버 역량 센터를 주최하는 유일한 국가로 글로벌 사이버 보안에 대한 기여도에서 가장 높은 점수를 획득

✓ 추가적인 평가요소로 디지털 및 필수 서비스의 보호를 포함하여 전자 서명에 영향을 미치는 신뢰 및 전자 식별 서비스도 포함

✓ 또한 개인정보 보호, 사고 및 위기관리, 대응 능력을 분석. 동 부문은 적절한 수준을 갖춘 국가가 없었으며 실제로 정부 단위의 대규모 사이버 사고에 대한 위기관리 계획이 부족

✓ 우루과이와 아이티의 경우 사이버 범죄 대응 부서가 부재

이 슈	주 요 내 용 및 시 사 점
	✓ 법령 부문에서 도미니카 공화국이 높은 점수를 받았으며 동 국가는 2018년 국가 사이버보안 전략을 수립하고 규제하는 법령 230-18의 틀 내에서 사이버 보안 전략을 발표 * 디지털 프로그램은 법령 258-16을 통해 만들어졌으며 4가지 목표, 13가지 구체적 활동 및 37가지 행동강령을 갖춤 * 4가지 목표 : 1) 법적 틀 및 제도적 강화; 2) 국가 중요 인프라 및 정부 IT 인프라 보호; 3) 국가 사이버 보안 교육 및 문화; (4) 국내 및 국제 파트너십 구축
[도미니카 공화국] 사이버 보안 연례보고서 발표	▸ **도미니카 공화국, 국가 사이버보안 센터(CNCS) 연례보고서를 통해 늘어난 랜섬웨어 공격 발표** ✓ 도미니카 공화국 국가 사이버보안 센터(CNCS)의 연례 보고서에 따르면 '22년 공동 호스팅 인프라를 공유하는 도미니카 공화국의 기관 정보 포털 총 46개 중 14개가 사이버 공격을 받았으며 '21년 50개에서 '22년 464개로 영향을 받은 국가 도메인이 증가 ✓ '22.8월 사이버 공격으로 Dominican Agrarian Institute(IAD) 시스템이 영향을 받았으며 2년 전인 '21.1월, 도미니카 통신 및 일반예산국(Digepres)과 통계청(ONE)이 영향을 받음 ✓ 중남미 지역을 타겟으로 한 랜섬웨어 공격이 증가하고 있으며, 동 공격으로 인한 위험성을 줄이기 도미니카 공화국은 긴급 조치, 우선순위 및 보완적인 추가 대책 마련의 필요성 강조 ✓ 중남미 지역 내 공공 부문 및 주요 인프라 부문 사이버 스파이 활동 및 정보 유출과 관련된 공격이 증가하고 있으며 국가들이 일반적으로 사이버 보안 사고에 대응할 계획을 가지고 있지만 역량 부족 ✓ 이용자, 민간, 공공 부문 전 분야에 걸친 디지털 의존성을 감안할 때 중남미 지역 내 사이버 보안 관련 이니셔티브, 전략, 정책 및 활동에 더 많은 노력과 자원 할당 필요 ✓ CNCS는 또한 랜섬웨어 위협을 효과적으로 방지, 탐지, 완화 및 대응하는 국가의 능력이 부분적으로 글로벌 파트너, 민간 부문, 시민 사회 및 일반 대중의 노력, 협력 및 탄력성에 달려 있음을 강조하며 사이버 복원력 강화 중요성을 강조
[콜롬비아] XMRig 오픈소스, 트로이 목마 Obot, Glupteba 봇넷이 위협적인 멀웨어로 언급	▸ **콜롬비아 역내 위협적인 멀웨어 3가지 종류 및 주의점 발표** ✓ Check Point Software Technologies Ltd.는 보고서를 통해 콜롬비아 내 위협적인 멀웨어 3가지 발표 ✓ 콜롬비아에서 연초에 가장 위험한 세 가지 멀웨어는 ▲Monero 암호 화폐를 채굴하는 데 사용되는 CPU 마이닝 소프트웨어인 XMRig 오픈 소스, ▲뱅킹 트로이 목마인 Qbot, ▲2011년부터 알려진 봇넷 Glupteba로 언급 ✓ 또한, 전 세계적으로 피싱 및 신용 도용 사례에 이용된 ▲Vidar Infostealer가 10위 안 ✓ Vidar Infostealer는 AnyDesk(원격 데스크톱 애플리케이션)와 연결된 가짜 도메인을 통해 확산하며 인기 애플리케이션의 URL 하이재킹을 사용하여 피해자를 회사의 공식 웹사이트를 시뮬레이션한 단일 IP 주소로 인도 ✓ 합법적인 설치 프로그램으로 가장하여 멀웨어를 다운로드하도록 유도하며 로그인 자격 증명, 비밀번호, 암호화폐 지갑 데이터 및 은행 정보와 같은 민감한 정보를 유출함

이 슈	주 요 내 용 및 시 사 점
	✓ 또한 중동 및 북아프리카 전역에 njRAT 멀웨어를 전달하는 ▲Earth Bogle이 확인됨. 공격자는 지정학적 피싱 이메일을 사용했으며 일단 다운로드 시 PC 트로이 목마 감염 및 민감한 정보를 훔치기 위해 수많은 침입 활동을 수행 ✓ 체크포인트 아메리카 대표인 Antonio Amador는 사이버 범죄 그룹은 개인정보를 훔치고 멀웨어를 확산시키기 위해 신뢰할 수 있는 계정 이름을 지속해서 이용한다고 언급 ✓ 이에 이용자가 URL 클릭 시 세심한 확인이 필요하다고 강조 ✓ 항상 최신 SSL 인증서가 있음을 나타내는 링크 옆의 보안 잠금장치를 확인하고 웹사이트가 악성임을 암시할 수 있는 숨겨진 오타 확인 필요
	▶ **시사점** ✓ 코스타리카 차베스 대통령은 지난달 랜섬웨어 공격 방어에 실패를 이유로 현지 과기부인 MICITT 장관을 교체한 것으로 추정 ✓ 새로운 장관 면담 등을 통해 코스타리카 SOC 구축 현황 등에 계획 확인 및 한국 기업 수주 가능성 논의 필요 ✓ 중남미 전역 사이버 보안 체계 마련에 대한 필요성이 강조되고 있으나, 국가 차원의 SOC 및 사이버 보안 역량 강화 프로그램 부재가 문제점으로 언급 ✓ KISA CAMP 및 GCCD를 통한 중남미 지역 사이버 보안 역량 강화를 위한 협력 강화 추진 필요

KISA 정보보호 해외진출 전략거점(중동) 2월 주요동향

2023. 02. 28(화), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[사우디] 제2회 미래 기술 컨퍼런스 개최	▸ **사우디 최대 기술 컨퍼런스 LEAP23 리야드에서 개최** ✓ 2023년 2월 6~9일 3일간 사우디아라비아의 수도인 리야드 국제 컨벤션 및 전시 센터(Riyadh International Convention and Exhibition Centre)에서는 제2회 미래 기술 컨퍼런스 LEAP23을 진행하고 관련 전문가들이 모여 토론에 참여 ✓ 올해 등록 건수는 250,000건 이상으로 작년 1회의 두 배 이상으로 세계에서 가장 빠르게 성장하는 기술 이벤트라고 평가 ✓ 전 세계적으로 기술 기반의 스타트업 및 중소기업은 일자리 창출과 성장, 혁신의 원동력으로 간주되며 LEAP는 전 세계적으로 스타트업이 참여할 수 있는 최고의 플랫폼 중 하나임 ✓ LEAP23에서 사우디 정보기술부 장관은 90억 달러 규모의 거래가 있었고 24억 3천만 달러 규모의 투자 프로그램을 발표 ✓ 신기술과 혁신적인 기술은 점점 더 삶의 모든 측면에 영향을 미치고 있으며 지속적으로 발전하고 개선되고 있으며 LEAP23은 이러한 최신 기술을 선보이고 있음
[오만] ICT 기술 투자 관련 국제 반도체 정상회의 개최	▸ **International Semiconductor Executive Summit 오만 무스카트에서 개최** ✓ 국제 반도체 최고 회의(International Semiconductor Executive Summit)가 2. 22~23 이틀간 Muscat에서 개최되었으며 이 행사는 오만 교통통신정보기술부가 개최 ✓ 이 행사에는 세계 여러 나라에서 동 분야 회사 전문가, CEO가 참여하여 오만의 정보 통신 기술(ICT) 투자 기회와 중동 및 북아프리카의 반도체 제조 과제를 포함하여 다양한 주제를 다룸 ✓ 오만 정부는 첨단 기술로 서비스 및 생산 부문을 디지털화하고, 통신 및 정보 기술 부문의 부가가치를 높이고, 총 경제에 대한 디지털 경제의 기여도를 높이는 것을 목표로 하는 디지털 경제로의 전환과 이를 통해 2040년까지 국내총생산(GDP)을 약 10%로 늘린 다는 계획 ✓ 오만 교통통신기술부는 오만의 디지털 투자기회 관련 발표를 하면서 우주 부문과 반도체 조립 및 유통 분야 외에도 데이터 센터, 클라우드 서비스, 멀티미디어, 콘텐츠 제작, 정보 통신 기술 서비스, 사이버 보안 등을 포함하며, 4차 산업혁명 기술 개발에 필요한 투자기회를 마련해야한다고 함 ✓ 오만은 네트워크 준비 지수에서 134개국 중 44위, 유엔 전자정부 개발 지수에서 193개국 중 50위에 올랐으며 100가구당 고정 광대역 가입자 수는 72%에 달하고 UN의 글로벌 사이버 보안 지수에서 175개국 중 21위를 차지했다고 함
	▸ **시사점** ✓ 사이버보안을 포함하는 신기술의 개발과 이에 대한 컨퍼런스를 활발히 개최하면서 다양한 투자기회를 마련 중