KISA 정보보호 해외진출 전략거점(동남아) 3월 주요동향

2023. 03. 31(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[베트남] 온라인 권리 보호	▸ **온라인 소비자 권리 보호** ✓ 산업통상부(MoIT)는 세계 소비자 권리의 날인 3월 15일을 소비자 권리의 날로 제정하고 올해는 정보의 투명성과 안전한 소비를 강조 ✓ 경쟁소비자청(Vietnam Competition and Consumer Authority)은 소비자 권리 보호에 관한 법률을 준비하고 5월 국회 본회의에서 의결될 예정 ✓ 2022년 위조 및 인증되지 않은 제품을 판매한 혐의로 기소된 5개의 전자상거래 웹사이트가 차단됨
[베트남] 사이버 공격 증가	▸ **베트남 사이버 공격 증가 및 사이버 사기 분석** ✓ 정보통신부(MIC) 산하 정보보안국(AIS)은 2월 IT 시스템에 문제를 일으킨 1,687건의 사이버 공격을 기록하였으며, 1월 대비 36.7%, 지난해 2월 대비 33.9% 증가하였음. 사이버 공격의 대부분이 사기성 웹사이트 및 링크인 피싱 공격임 ✓ 2022년에 개인정보 탈취를 위한 스캠과 금융 스캠이 주공격으로 12,935개의 온라인 스캠 사건을 발견 ✓ 브랜드 위조 72.6%, 온라인 계좌 도용 11.4%, 온라인 사기 스캠 및 렌딩 앱 등이 16%임 ✓ 베트남의 사이버 공간에 대한 감독을 강화하고 능동적 스캔, 레벨 기반 정보 보안 식별 및 구현을 위한 지원 플랫폼, 해외 베트남 정보보안 전문가 네트워크 배치 및 CCTV에 대한 보안 기준 등을 마련
[말레이시아] 사이버보안 대비 태세	▸ **사이버 위협 증가에 따른 기업의 사이버 보안 대비 태세** ✓ 통신 및 디지털부 차관은 최근 사이버 보안 공격의 빈도와 심각성이 증가하고 있다고 발표. 작년에 랜섬웨어 공격, 사이버 스파이, 데이터 유출 및 사이버 사기 등의 사건을 경험하였으며 4,741건의 사이버 위협 사례를 보고 ✓ Kaspersky에 의하면 2022년에악성 이메일 첨부 파일이 1,800만개 증가했음. 이는 2021년에 2.62% 증가, 2022년에는 3%로 증가하는 추세임 ✓ 정부는 #BeCyberSmart 캠페인을 통하여 사이버 보안에 대한 시민의 인식을 제고하고 PROTECT 360의 완전한 보안, 기기의 개인정보 보호 및 신원 보호, 맬웨어, 피싱 및 해킹 시도에 대한 보호를 제공 ✓ CISCO의 사이버 보안 준비 지수 보고서에 의하면 16% 기관만이 성숙 단계인 것으로 조사되어 사이버 공격에 대비하고 있는 것으로 조사되었음 ✓ 더불어 95%의 응답자는 향후 12 ~ 24개월 내에 사이버 공격이 있을 것으로 예상하며 55%의 응답자는 지난 12개월 내에 사이버 공격을 경험한 것으로 답변하였음
[말레이시아] 사이버보안 침해사고 및 정부 대응	▸ **말레이시아 정부의 사이버 보안 조직 개편 및 예산 증가** ✓ 통신 및 디지털부 장관은 말레이시아 사이버 보안 위원회 설립을 제안하여 관계부처와의 협의를 거쳐 6월 국회에 상정될 예정임을 발표. 새로이 설립되는 사이버보안 위원회의 설립은 1 ~ 2년이 소요될 예정임

이 슈	주 요 내 용 및 시 사 점
	✓ CyberSecurity Malaysia(CSM)가 수행하는 사이버보안 임무의 기능 또는 관할권을 계속될 것임을 발표 ✓ 또한 양자 암호를 포함한 데이터 보안의 핵심인 암호화 정책을 새로이 수립할 예정임을 발표 ✓ CSM의 CEO는 NSRC(National Scam Response Center)의 온라인 사기 또는 사기를 퇴치하기 위하여 RM1000만을 할당한다고 발표. CSMdms Cyber999를 통하여 사이버보안 사고 보고서를 받으며 이의 70% 이상이 온라인 사기와 관련이 있다고 함
[필리핀] 사이버보안 대비 태세	▸ **필리핀 기관의 27%만이 사이버 공격을 막을 수 있는 준비 태세 갖춤** ✓ CISCO의 사이버보안 준비 지수 보고서에 의하면 27% 기관만이 성숙 단계인 것으로 조사되어 사이버 공격에 대비하고 있는 것으로 조사되었음 ✓ 더불어 85%의 응답자는 향후 12 ~ 24개월 내에 사이버 공격이 있을 것으로 예상하며 77%의 응답자는 지난 12개월 내에 사이버 공격을 경험한 것으로 답변하였음

KISA 정보보호 해외진출 전략거점(북미) 3월 주요동향

2023. 03. 31(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[미국] 경제 상황이 악화됨에 따라 일부 보안 스타트업은 '시장이 모든 혁신을 흡수할 수 없다'는 냉엄한 현실에 직면했음	▸ **사이버보안 스타트업이 너무 많으며, 일부는 경기 침체에서 살아남지 못할 것** ✓ 사이버보안 부문은 작년에 시작된 경제 위기 이후 상당히 견고해 보였음. 예를 들어 사이버보안 시장에 있는 수천 개의 공급업체 중 일부만이 대규모 해고 ✓ 하지만 앞으로 몇 달 안에 더 많은 균열이 나타날 가능성이 있으며, 사이버보안 산업은 경기 침체 기간 동안 많은 공급업체를 어느 정도 온전하게 유지하는데 도움이 될 것으로 기대 ✓ 이러한 힘에는 랜섬웨어, 데이터 갈취 및 국가 위협과 같은 성가신 문제는 말할 것도 없고 정부 규제 기관 및 사이버 보험사의 계속 증가하는 요구사항 목록이 포함됨 ✓ 그러나 이 시점에서 사이버보안 도구에 대한 일정 수준의 수요가 본질적으로 내장 되어 있지만 특정 보안 신생 기업을 다른 부문의 상대보다 실패 위험이 더 큰 한 가지 독특한 요소가 있음 ✓ 온라인 사이버보안 데이터베이스인 CyberDB는 현재 3,000개의 보안 공급업체를 집계하고 있으며, 그 중 소수는 대규모 "플랫폼" 회사임 ✓ 나머지는 보다 제한된 제품 기능 세트를 제공하고 있음 ✓ 무엇보다도 이 공간에 있는 회사의 과잉은 사이버보안 복잡성과 "도구 확산"이라는 널리 알려진 문제를 악화시켰음 ✓ 이제 본격적인 경기 침체에 대한 두려움이 커지면서 많은 사이버보안 공급업체가 취약할 수 있다는 우려도 커지고 있음 ✓ 사이버보안 산업을 처음으로 만든 주요 기업가 중 한 명인 Gil Shwed에 따르면 의심할 여지없이 현재 시장에는 벤더의 "과부하"가 있음 * Shwed는 최신 방화벽을 구현하는 데 중요한 역할을 했으며 1993년에 Check Point Software Technologies를 공동 설립 ✓ 이스라엘에서 사이버보안 스타트업의 물결을 목격한 Shwed는 최근 CRN에 도전적인 경제 환경과 넘쳐나는 보안 벤더가 문제라고 말함 ✓ 그는 "시장의 합리화를 보게 될 것"이라고 말했으며, "불행하게도 우리는 이미 그 중 일부를 보기 시작했음. 생존 가능한 공급 업체가 될 수 있는 비즈니스 모델을 구축하지 않았기 때문에 살아남는 데 어려움을 겪는 회사들임" ✓ 즉, 일부 보안 공급 업체는 비즈니스를 유지하기 위해 이익을 내야 할 때 그렇게 하지 못할 수 있으며, 그리고 모든 사람이 인수자를 반드시 찾을 수 있는 것은 아님 ✓ 이스라엘 이메일 보안 벤더 사이렌(Cyren)은 2월22일 운영을 중단하고 자산 청산을 추진할 것이라고 발표 ✓ 32년의 상장 기업인 이 회사는 "현재 시장 상황 및 추가 자본 조달과 관련된 문제"와 구매자를 찾을 수 없는 상황을 언급했음 ✓ 위협 인텔리전스 회사인 GreyNoise의 설립자이자 CEO인 Andrew Morris는

이 슈	주 요 내 용 및 시 사 점
	지난주 트윗에서 “올해 많은 사이버 보안 회사가 실패할 것”이라고 언급 ✓ 모리스는 트윗에서 “그들은 돈이 부족해 문을 닫거나 사모펀드 자산 매각에 들어갈 것”이라고 말함 ✓ 이것은 의심할 여지없이 단기적으로는 고통스러울 것이지만 “중장기적으로는 업계에 좋은 일”이라고 표현 ✓ 모리스는 “이들 회사 중 다수는 저렴하거나 무료인 외부자본으로 연명해 왔다”며 “사이버보안 기술을 실사하는 데 믿을 수 없을 정도로 경험이 없는 순진한 VC의 새로운 물결”을 포함 ✓ 특히, 사이버보안 회사에 대한 VC 자금은 2022년에 전년도 사상 최고치에서 37%급감했으며, 이는 반가운 변화라고 할 수 있음 ✓ 벤처 기업 Night Dragon의 전무이사인 Morgan Kyauk는 CRN과의 이전 인터뷰에서 경제 침체 이전에 “반드시 회사가 아니어야 했던” 많은 사이버 보안 스타트업이 VC 자금을 조달했다고 말함 ✓ CRN과의 대화에서 Shwed는 실패한 스타트업에 이르게 된 모든 사람에 대해 확실히 느낀다고 말했음 ✓ “저는 기업가이기 때문에 기업가가 꿈을 잃는 것을 보고 싶지 않습니다. 사람들이 일자리를 잃는 것을 보기 싫고, 긍정적으로 보는 건 아니다” 라고 표현 ✓ 그러나 Shwed는 사이버보안 산업이 단순히 “너무 많은 혁신”이 있었던 지점에 도달했다는 사실이 남아 있다고 말했음 ✓ 현재 상태로는 “시장이 모든 혁신을 흡수 할 수는 없습니다.”라고 말했으며, “좋은 아이디어, 좋은 사람, 좋은 기술이 있음. ✓ 하지만 고객이라면 매년 300개의 기술을 검토할 수는 없을 것임
[미국] Saltzman 우주작전 책임자는 우주군이 사이버보안을 위한 ’24년 예산에서 7억 달러를 모색하고 있음을 밝힘	▸ **미국 우주군, 사이버보안 지출 확대** ✓ 미국 우주군의 수장인 Chance Saltzman 장군은 3월 28일 국회의원들에게 우주군이 증가하는 위협에 대응하여 위성 지상 시스템을 위한 사이버보안에 막대한 투자를 하고 있음을 밝힘 ✓ 하원 세출 위원회의 국방 소위원회 청문회에서 우주 작전 책임자인 Saltzman 장군은 위성 시스템이 사이버 공격의 표적이 된 것을 목격한 러시아의 우크라이나 침공 이후 더 큰 보호의 필요성이 강화 되었다고 말했음 ✓ 2024년 회계연도에 대한 우주군의 300억 달러 예산 요청에는 우주 작전과 관련된 중요한 네트워크의 사이버 방어를 강화하기 위한 7억 달러가 포함되었다고 Saltzman 장군은 말함 ✓ “우주가 미래에 효과적인 운영의 중심이 될 것이라는 데는 의심의 여지가 없음”이라고 그는 말했음 ✓ 침공 초기에 러시아의 전자 및 사이버 공격은 경종을 울렸다고 말함 ✓ Saltzman은 2024년 요청에는 어떤 사이버 보안 기능에 자금이 지원되고 있는지에 대한 세부 정보를 제공하지 않음 ✓ 그는 우주군이 소프트웨어와 하드웨어뿐만 아니라 운영자 교육에도 투자하고 있다고 말했음 ✓ Frank Kendall 공군장관은 세출 청문회에서 美 국방부가 역사적으로 SW 개발에서 경험한 더 큰 문제로 인해 사이버 방어를 업그레이드하는 것은 우주 프로그램에 대한 도전이었다고 말함

이 슈	주 요 내 용 및 시 사 점
	✓ 눈에 띄는 예는 공군이 몇 년 전에 Global Positioning System 위성 별자리를 위해 개발하기 시작한 지상 제어 시스템이며, 이 시스템은 프로그램에 삽입되고 원래 소프트웨어에서 설계되지 않는 사이버 보안 기능으로 인해 부분적인 지연으로 인해 어려움을 겪음 ✓ 국방 세출 소위원회의장인 Ken Calvert(공화당/캘리포니아)는 가장 문제가 많은 우주군 프로그램이 지상 시스템이라고 지적했음 ✓ Kendall은 Frank Calvelli 우주군 인수 책임자가 작년에 취임한 이후 지상 시스템 개발에 대한 새로운 접근 방식을 요구했음 ✓ Calvelli는 발사 전에 지상을 제공하고 있는 지상 시스템이 완료 되고 새로운 기능을 발사하기 전에 작전 준비가 되도록 보장하도록 하고자 함
	▸ **시사점** ✓ 미국 시장의 경제 상황 악화로 인해 스타트업에 대한 투자가 향후 감소 할 것으로 예상되며, 이에 대한 국내 스타트업에 대한 투자 역시도 어려울 것으로 예상됨 ✓ 이러한 부분에 대한 대응을 위해 스타트업에 대한 지원에 대해 정부 차원의 다양한 역량 강화가 필요함 ✓ 미국은 우주군에 대한 보안 시스템 강화에 대한 기술 및 투자 부분에 대한 노력을 하고 있으며, 대한민국 역시 이러한 부분에 대한 노력이 필요 ✓ 향후 대한민국도 우주 기술에 대한 연구와 함께 정보보호에 대한 관심을 갖고 이에 대한 정책 및 투자에 대한 노력을 해야 함

KISA 정보보호 해외진출 전략거점(아프리카) 3월 주요동향

2023. 3. 31(목), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[나이지리아] 대선 기간 1,300만 건의 사이버 공격 기록	▸ **공공 웹사이트 및 포털 포함 사이버 공격 급증(1,300만건)** ✓ 나이지리아 대선 기간 동안 나이지리아 내외에서 다수 사이버공격 발생 * 대선일 당시 공공 웹사이트 및 포털 공격 건수: 약 700만 건 ✓ 사이버 공격 차단 및 적절한 예방 조치를 위해 관련 기관에 노력 지시 ✓ 사이버공간 및 ICT 인프라 보호를 위한 자문 역할 담당 위원회 발족 등 국가적 노력 中
[케냐] E-citizen 플랫폼 서비스 개시 후 세수 증대	▸ **정부의 대국민 서비스 디지털화 이후 급증된 세수 확보** ✓ E-citizen 플랫폼 서비스의 디지털화를 통한 세수는 1억 실링 이상(일일 기준) * 정부의 세수 확보 노력과 함께 서비스 접속자 수는 증가 중(현재 53백여대 이상) ✓ 모바일기기 등 온라인을 통한 출생 및 결혼 증명서 발급 등 대표적 사례 이용 ✓ 전자플랫폼 서비스를 통해 새로운 일자리 창출 등으로 청년층 경제의 긍정적 효과 발생
[르완다] ICT를 통한 강력한 디지털 거버넌스 구축	▸ **르완다의 디지털 거버넌스 구축 및 데이터 보호 필요성 증가** ✓ ICT를 통한 거버넌스 구축 이후 늘어난 데이터의 관리 중요성 및 효율적 이용 등의 체질 변화에 대한 요구가 크게 증가 ✓ ICT혁신부의 유엔 경제사회부(UN DESA)와의 협력 추진 등 역량 개발에 집중 * 대국민 서비스의 온라인 전환 완료 목표('24년)와 4G 인프라 투자 강화 추진 ✓ 디지털 인프라 개발 지수 향상 및 대국민 서비스의 완전 온라인화 전환 등 ICT 거버넌스는 시민의 보안과 프라이버시 보장을 함께 고려하여 개발할 필요
[가나] 개인정보 보호 관련 포털 서비스 개시	▸ **정보서비스부의 개인정보 오남용 방지 관련 포털서비스 개시** ✓ 개인정보의 오남용 및 허위정보 퇴치 등 정부 차원의 데이터 보호 서비스 실시 * 본 서비스를 통한 정부 ICT 및 정보보호 프로그램 재조직과 개편 등에 영향 ✓ ICT 전환 이후 미디어 및 소비패턴의 변화로 다양한 정부서비스 출범을 앞당기는 계기였으며, 다양한 정보에 따른 대국민 서비스 개선을 목표함 ✓ 대국민 서비스 개선 시 개인정보의 오남용 및 허위정보 방지 등 정보보호 노력이 필수라는 인식과 함께, 사이버범죄에 대한 강력한 대응 예고
	▸ **시사점** ✓ 아프리카 국가는 정부 관련 정보보호 프로젝트가 다수 발굴되는 추세. ✓ 대선 전후 사이버공격 증가 등 온라인 대상 정보보호 필요성이 자주 언급되며, 탄자니아의 경우 대선 직후 디지털 포렌식을 도입하는 등 정보보호 프로젝트 발굴 기회 증가 中 ✓ 당 거점은 정부 차원의 정보보호 프로젝트 발굴 집중 등 고려 필요

KISA 정보보호 해외진출 전략거점(중남미) 3월 주요동향

2023. 03. 31(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[페루] Fortinet 최신 사이버 공격 분석 보고서 발표	▸ **Fortinet 보고서, 페루 대상 사이버 공격('22, 150억 건) 발표** ✓ 네트워크와 보안의 융합을 주도하는 글로벌 사이버 보안 리더인 Fortinet에서 최신 반기별 글로벌 위협 환경 보고서 발표 ✓ 데이터에 따르면 페루는 2022년에 150억 건의 사이버 공격 시도를 받았으며 이는 2021년 대비 35% 증가한 수치 ✓ 라틴 아메리카 및 카리브해 지역은 2022년에 3,600억 건 이상의 사이버 공격 시도를 겪음. 멕시코가 가장 많은 공격 시도(1,870억 건)를 받았으며, 브라질(1,030억 건), 콜롬비아(200억 건), 페루(150억 건)가 그 뒤를 이음 ✓ FortiGuard Labs의 수석 보안 전략가이자 위협 인텔리전스 글로벌 부사장인 Derek Manky는 사이버 공격 및 비정상적 접근을 탐지하기 위한 기술이 발전하는 만큼 사이버 공격자 또한 더 정교한 와이퍼 멀웨어 또는 지능적이고 지속적인 위협 방법으로 공격을 수행하고 있다고 언급 ✓ 이러한 지능형 사이버 범죄 전술로부터 보호하기 위해 모든 보안 장치에서 실시간 머신러닝으로 구동되는 위협 인텔리전스를 활성화하여 의심스러운 작업을 감지하고 확장된 공격을 완화하기 위한 노력이 필요 **<2022년 하반기 보고서 주요 내용>** - **와이퍼 맬웨어***의 대규모 배포는 사이버 공격의 진화를 보여줌 * 와이퍼 맬웨어 : 파일이나 디스크를 완전히 삭제함으로써 컴퓨터 시스템이 제대로 작동하지 못하게 하는 악성 소프트웨어 - **랜섬웨어 위협**은 RaaS(Ransomware-as-a-Service)에 의해 활성화된 새로운 변종과 함께 서비스 속도를 지연시키는 등 최고 수준을 유지 - **코드 재사용** 등을 통해 효율성과 경제성을 보장한 **1년 이상 된 맬웨어**가 가장 활성화됨 - **Log4j**는 모든 지역 및 산업, 특히 기술, 정부 및 교육과 같은 부문의 조직에 지속적으로 영향을 미치고 있음 ✓ 와이퍼 악성코드 데이터를 분석한 결과, 사이버 공격자들이 공격 대상에 대해 이용 기술 추세를 분석 가능. 또한 경계가 없는 인터넷을 통해 사이버 범죄자는 주로 CaaS(Cybercrime-as-a-Service) 모델을 통해 공격 확장 ✓ FortiGuard Labs Incident Response(IR) 보고서에 따르면 금전적 동기가 있는 사이버 범죄가 가장 많은 사건(73.9%)을 발생시켰으며 2위는 스파이 활동(13%)으로 분석 ✓ 2022년, 금전적 동기가 있는 사이버 범죄 중 82%가 랜섬웨어 또는 악성 스크립트의 사용과 관련되었으며, 랜섬웨어 중에서도 서비스형 랜섬웨어(Ransomware -as-a-Service)의 이용이 전 세계적으로 증가 ✓ 사이버 공격자는 조직화 되고 기존 경험을 기반하여 공격을 통한 수익성을 확대 ✓ 코드 재사용은 범죄자가 성공적인 결과를 기반으로 공격을 미세 조정하고 방어 기술을 피하기 위해 효율적이고 수익성 있는 방법

이 슈	주 요 내 용 및 시 사 점
	✓ 사이버 범죄자는 위협을 자동화할 뿐만 아니라 코드를 적극적으로 업데이트하여 더욱 효과적으로 공격 시도 ✓ 코드 재사용 외에도 공격자는 기존 인프라와 오래된 위협을 활용하여 기회를 극대화함. 봇넷 위협을 조사할 때 상위 봇넷 중 상당수는 새로운 것이 아니며 "오래된" 봇넷은 여전히 매우 효과적으로 판명 ✓ 구체적으로 2022년 하반기 범죄자들은 입증된 방법을 사용하여 MSSP (Managed Security Service Providers), 통신 부문, 보급형 운영 기술(OT)로 유명한 제조 부문을 표적으로 삼기 위해 노력하고 있음 ✓ Log4j는 2021년 및 2022년 초, 위험성이 널리 알려졌음에도 불구하고 상당수의 조직이 적절한 보안 제어 패치를 구현하지 않음에 따라, 2022년 하반기에도 Log4j는 모든 지역에서 여전히 매우 활동적으로 위협을 가함 ✓ 공격자는 주로 이용자가 인터넷을 서핑하고 손상된 웹 사이트를 방문하거나, 악성 이메일 첨부 파일을 열고, 사기성 링크 또는 팝업을 클릭하여 의도하지 않게 악성 페이로드를 다운로드할 때 피해자의 시스템에 접근 가능. 문제는 악성 페이로드에 접근 및 다운로드가 일어나면 피해 복구가 어려움 ✓ 위협 해결을 위해 Fortinet은 CISO와 보안 팀이 일련의 공격을 차단하고 보안 사고의 영향을 최소화하며 잠재적인 사이버 위협에 더 잘 대비할 수 있도록 보안 솔루션을 제공 ✓ Fortinet은 NGFW(Next Generation Firewalls), 네트워크 원격 측정 및 분석, EDR(Endpoint Detection and Response), XDR(Extended Detection and Response), DRP(Digital Risk Protection), 보안 정보와 같은 다양하고 강력한 도구 및 이벤트 관리(SIEM), 온라인 샌드박싱, 디셉션, 보안 오케스트레이션, 자동화 및 대응(SOAR) 등 보안 사고를 신속하게 감지하고 대응하는 데 도움이 되는 고급 위협 감지 및 예방 관련 솔루션을 제공
[코스타리카] MICITT, 사이버보안 중요성 강조	▸ **MICITT, 새로 임명된 장관, 사이버보안 중요성 강조** ✓ 새로 부임한 Paula Bogantes 장관은 사이버보안이 MICITT의 주요 우선순위임을 표명 ✓ 1월 24일부터 MICITT에는 새로운 리더, 새로운 경영진이 발탁되었으며, 새 장관은 사이버보안 및 디지털 거버넌스 문제가 우선순위임을 명확히 함 ✓ 이전 디지털 정보 국장(Paula Brenes Ramirez)은 사이버보안 도구 툴 도입에 대해 새로 임명된 장관과 의견 마찰을 보임 ✓ 새로 부임한 장관은 "MICITT이 과학, 기술, 혁신, 통신 등 여러 주제를 다루고 있으나, 우선순위 중 하나는 사이버보안이 될 것이며, 또 다른 사이버 공격의 희생자가 되기 전에 가능한 한 빨리 새로운 전략을 구현해야한다 "고 강조 ✓ 장관은 "우리가 가진 장점 중 하나는 사이버 보안 문제의 선도적인 다국적 기업이 코스타리카에 지원을 하고 있으며, 선도적인 전략적 파트너 지원을 통해 공격을 예측하는 데 도움이 될 수 있다“라고 언급 ✓ 또한, 사이버보안법이 지속 논의되어야 하며 사이버보안 전문 지식을 갖춘 “Cybersecurity Agency” 정부 기관 설립 필요성을 강조
[코스타리카] MICITT, SOC 서비스 아웃소싱 고려	▸ **MICITT, SOC(보안관제센터) 운영을 위한 아웃소싱 가능성** ✓ 코스타리카 과기부(MICITT)는 ’22년 사이버 공격으로 인한 국가 비상사태에 직면하여 제안된 주요 해결책 중 국가 SOC 설립을 포함

이 슈	주 요 내 용 및 시 사 점
	✓ 전 MICITT 장관의 추정에 따르면 센터 구축에 필요한 금액을 10억 콜론으로 발표 ✓ 예산에는 24시간 탐지 활동을 위한 교육, 라이선스, 소프트웨어 등이 포함 ✓ 현재 코스타리카 MICITT 내 컴퓨터 보안사고 대응 센터(CSIRT-CR)가 있으며 높은 초기 투자를 고려 시, 다른 방안이 논의되고 있음 ✓ 새로 부임한 Paula 장관은 국가 역량 내에서 SOC를 구축하고 국가가 사이버 보안 역량을 갖추어야 한다 생각함 ✓ 다만, 시간이 소요되는 만큼 SOC 구축 전까지 SOC를 위한 서비스 아웃소싱을 해결방안으로 고려하고 있다고 발표 * 지침 No. 46-H-MICITT은 공공 부문 기관 필요한 경우, 클라우드 컴퓨팅 솔루션을 획득할 수 있다고 규정하고 있음. 이는 컴퓨터, 라이센스, 컴퓨터 시스템, 웹 페이지 호스팅 서버, 앱 서버, 이메일, 방화벽, 운영 체제, 데이터베이스 또는 기타 유형의 기술 개발을 위한 기타 컴퓨터 기술 등에 적용 ✓ 이런 경우, MICITT은 서비스 솔루션을 제공하는 사이버보안 회사를 통해 초기 정부의 투자 및 후속 유지 관리 비용을 들이지 않고 사이버 위협에 대한 월별 요금을 지불할 수 있다고 현지 언론은 보도 ✓ 이에 보안, 인텔리전스 및 사이버 위협의 솔루션을 갖춘 현지 기업들이 관심 표명 ✓ 특히, 콜롬비아 회사인 MULTISOFT는 2~5년 안에 코스타리카에 SOC 구축 등을 포함한 계획에 백만달러를 투자하고 코스타리카 지역에서 중앙 집중화 가능한 서비스 허브를 구축한 후, 다른 국가로 사업을 확장하고 싶다고 표명
[중남미] 2030년까지 중남미 지역 사이버보안 시장 확대	▸ **Quadintel, 중남미 사이버보안 시장에 대한 새로운 연구 보고서 발표** ✓ Quadintel(시장 조사 보고서 회사)에서는 중남미 사이버보안 시장 전망, 성장, 비용 구조, 수익, 시장 동향(2023-2030)에 대한 분석 보고서 발표 ✓ 또한, 여러 시장 범주에 걸쳐 라틴 아메리카 사이버보안 시장에 대한 포괄적인 범위, 국가 수준의 심층 연구, 시장의 주요동인, 제한 사항, 추세 및 기회에 대한 평가를 제공 ✓ 중남미 사이버 보안 시장은 연평균 12.3% 성장률(CAGR)로 성장할 것으로 예상되며 23년 미화 65억 2023천만 달러의 가치 시장을 달성할 것으로 예측 ✓ 중남미 사이버 보안 시장에서 Symantec, Avast, McAfee, Trustwave, CA Technologies, Kaspersky Lab 등이 주요 사업자로 분석 됨 ✓ 2016년 중남미 사이버 보안 시장에서 전 세계 매출의 7.9%만 차지하였으나, 대부분의 나라가 취약한 사이버 보안 인프라를 갖추고 있다보니 보안 소프트웨어 제공 업체에게 중남미 시장은 매력점임 ✓ 국가별로 중남미 사이버 보안 시장은 브라질, 멕시코, 아르헨티나 및 기타 사이버 보안 시장으로 분류됨 ✓ 브라질은 중남미 지역에서 가장 큰 경제 국가로 동 국가는 인구의 50% 이상이 인터넷 접속이 가능해짐에 따라 디지털 혁명을 겪고 있음 ✓ 또한 2016년 하계 올림픽 기간 동안 심각한 사이버 공격으로 국가 이미지가 실추된 후, 사이버 보안의 중요성이 증가함에 따라, 관련 사이버보안 시장이 확대됨 ✓ 중남미 지역 사이버보안 솔루션은 ID 및 접근 관리, 암호화, 거버넌스 규정 및 규정 준수, 통합 위협 관리, 보안 정보 및 이벤트 관리로 분류됨 ✓ 식별 및 접근 관리가 가장 주요하게 인식되고 있으며 디지털 신원 관리에 대한 국가 전략이 부재함에 따라, 현재 브라질 내 전자 정부 서비스는 ID 관리 관련하여 문제에 직면

이 슈	주 요 내 용 및 시 사 점
	<주요 성장 요인> - 중남미 지역 내 디지털 경제가 성장함에 따라 국가는 사이버보안 정책을 업데이트하고 개인정보를 보호하기 위한 필수적인 기술적 조치 마련 필요 - 중남미 지역 내 모든 서비스들이 IoT화되고 있음
[콜롬비아] 사이버 보안 관련 예산 증액	▸ **콜롬비아 정부, 사이버보안 관련 예산 100억 달러 증액** ✓ 콜롬비아 산드라 밀레나 우루 티아 ICT 장관은 “사이버 보안은 모든 시민을 위한 업무이다"라는 강력한 메시지를 수도에서 열린 "사이버 보안의 과제" 회의에서 발표 ✓ 장관은 이번 정부가 조치한 디지털 보안 강화를 위한 활동을 발표. 특히, 작년 Colcert에 할당된 예산이 30억 달러에서 금년 100억 달러로 증액되었으며, 이를 통해 오늘날 당면한 위기에 맞서 역량을 강화할 준비가 되었음을 강조 ✓ Colcert는 콜롬비아의 사이버 비상 대응 그룹으로, 공공 및 민간 부문 모두에서 국가 디지털 보안 사고에 대한 예방, 완화, 관리 및 대응을 조정하는 연락 창구이며 작년에 동 기관은 287건의 사건 분석하고 2023년 15건의 사건을 해결 ✓ 장관은 콜롬비아의 신뢰할 수 있고 안전한 디지털 생태계 구현 촉진 및 국가, 시민 및 민간 부문 보호를 위해 국가 디지털 보안국(National Digital Security Agency)의 창설이 국가 개발 계획에 포함되었음을 강조
[온두라스] 사이버 보안 관련 법률 제정 권장	▸ **온두라스, 전문가들은 정부에 사이버보안 전략 및 법률을 마련할 것을 권고** ✓ 코로나19 팬데믹 이후 기업과 개인에 대한 사이버 공격이 전 세계적으로 증가하고 있으며, 많은 사람들이 인터넷 접속 및 재택근무를 시행 ✓ 동 상황에 직면하여 지역의 여러 국가에서는 시민을 보호하려는 법률과 규정을 통해 사이버 보안 조치를 취했으나, 온두라스는 관련된 조치가 미흡 ✓ 매일 수백 명의 온두라스 시민들은 사용자와 기업의 개인정보를 유출하려고 하는 악성 문자 메시지와 이메일에 노출되고 있으며 이는 금전적 피해로 연결 ✓ 전문가들은 사이버 범죄 집단으로부터 시민의 데이터 보호, 조사 및 기소를 진행하기 위해 법적 규정이 필요하다고 호소 ✓ 특히, 가장 사이버공격을 많이 받고 있는 은행의 경우, 대응력이 강화되어 있으나, 교육 기관과 제조 회사 또한 지속적인 공격에 노출되어 있다고 사이버 보안 회사인 Sisap의 Utrera가 언급 **<전략>** ✓ 온두라스 내에서 사이버 보안법을 제정하려는 시도가 있었으나, 여전히 진행에 어려움이 있음. 특히 2021년 인터넷 거버넌스 포럼(IGF) 온두라스 지부에서 사이버 범죄를 유형화하고 피해자를 보호하기 위해 동 보안법 필요성이 논의 ✓ 온두라스 내, 사이버 범죄 관련 교육 및 예방 강화를 위한 기관의 CEO인 Sandy Palma는 "온두라스는 국가 사이버 보안 전략이나 공공 사이버 보안 정책 또는 국가 사이버 보안법, 세 가지 중 하나를 마련하고, 관련 내용을 형법에 포함하여 사이버 범죄 관련 법률 마련, 사이버 범죄 조사를 위한 검찰청의 창설, 사법 운영자 교육 및 보안 운영을 위한 센터 설립"이 필요하다고 강조 ✓ (권장 사항) 사이버 위험 노출의 최소화를 위해 ▲신원 미상으로 받은 이메일이나 링크를 클릭하지 않고, ▲모든 프로그램에 동일하지 않은 보안

이 슈	주 요 내 용 및 시 사 점
	이메일 비밀번호를 사용하며, ▲소셜 네트워크에서 알 수 없는 사람을 추가하지 않는 것을 권장 ✓ (사이버 대응 센터 창설) 또한 사이버 보안 문제를 교육 커리큘럼에 포함하고 온라인 폭력에 대한 법률 제정 및 금융, 정부, 공공 및 민간 부문을 위한 컴퓨터 사고 대응 센터를 창설할 것을 권고 ✓ 위 권장 사항은 당국에 제출되었으나, 정부 측으로부터 회신이 없음 ✓ ESET의 최신 보안 보고서에 따르면 2021년 중미 기업을 대상으로 한 약 2.1백만 건의 사이버 공격이 탐지되었으며 그 중 43만건이 온두라스에서 탐지 되었다고 발표 ✓ 피싱 이메일을 통해 사이버 범죄자는 피해자에게 사기성 웹 사이트 상, 민감한 개인정보를 업데이트하도록 유도하고 문자 메시지를 통해 기밀 정보를 얻으려고 하는 "스미싱" 기법, 사이버 범죄자가 감염된 컴퓨터나 시스템을 제어하고 다양한 방법으로 하이재킹하여 정보를 암호화하고 화면을 차단한 랜섬웨어가 성행 ✓ 전문가들은 이를 개선하기 위한 국가 전략 및 법률 마련이 시급함을 강조
[온두라스/코스타리카] 한국 전자정부 사절단과 포럼 개최 및 사이버보안 부문 논의	▸ **온두라스(3.20), 코스타리카(3.22) 한국 전자정부 사절단과의 협력 포럼 개최 및 사이버보안 부문 실무 협력 양자회담 개최** ✓ 디지털 정부의 발전을 촉진하고 경제 성장 및 기술 등 지식공유를 위해 한국 행안부와 코스타리카 MICITT 정부 간 MoU 체결 ✓ 동 MoU는 워크숍, 포럼 및 공동 세미나 개최, 컨설팅 서비스 및 디지털 정부 문제에 대한 프로젝트 개발을 통해 국가 차원의 역량 구축에 기여할 것으로 예상 ✓ 특히, 한국은 약 1만 달러를 코스타리카에 기부할 것이며, 동 기금을 통해 공공 부문의 디지털 전환 프로세스에 대한 제안 및 솔루션 등이 진행될 것으로 예상 ✓ 또한, 한국 전자정부 사절단은 행안부, 국세청, 관세청, 조폐공사, NIA, KISA 등 전문가와 함께 온두라스 및 코스타리카에서 전자정부 협력 포럼을 개최하고 전자정부, 디지털 신원, 사이버보안 등에 대해 논의
	▸ **시사점** ✓ 코스타리카 과기부에 새로 부임한 Paula 장관이 사이버 보안을 우선순위로 두고 향후 사이버보안 센터 설립 필요성 등 적극적인 행보를 보이고 있음 ✓ 다만, 제대로 된 전략이 마련되기 전까지 다국적 사이버보안 기업을 대상으로 아웃소싱을 받고자 하는 움직임이 있으며 콜롬비아 등 여러 기업에서 관심을 보이고 있음 ✓ 중남미 전역에 국가 사이버 보안관제 센터 설립 및 관련 법률, 정책 마련 필요성이 강조되고 있음 ✓ 한국기업 대상 관련 현지 동향을 전달하고 한국 정부 지원금 및 중남미 거점 지원 등을 통해 중미 진출을 하고자 하는 한국 기업에 적극적 지원 필요

KISA 정보보호 해외진출 전략거점(중동) 3월 주요동향

2023. 03. 31(금), 한국인터넷진흥원 보안산업단 글로벌협력팀

이 슈	주 요 내 용 및 시 사 점
[UAE] 제11회 사이버 보안컨퍼런스 GISEC 개최	▸ **UAE GISEC 2023 두바이에서 개최** ✓ Dubai World Trade Center과 UAE Cybersecurity Council이 주최하는 제11회 GISEC Global 2023이 3월 14일~16일에 두바이에서 개최 ✓ 500개 이상의 사이버보안 기업, 300여명의사이버 보안 발표자 및 토론자 등 세계 최고의 보안 전문가 들이 참여하여 글로벌 보안 동향 및 시장에 대해 논의 ✓ 이 행사는 공식 정부 사이버 보안 파트너인 두바이 전자 보안 센터(DESC), 내무부, 통신 및 디지털 규제청(TDRA), 두바이 경찰 등이 참여 ✓ GISEC 글로벌 2023은 데이터 관리, 사이버보안, 정부 서비스 및 거버넌스의 디지털 전환에 대한 UAE의 목표를 달성하기 위해 개최 ✓ 중동, 아프리카 및 아시아 전역의 주요 기업의 CISO가 참석하였고, 정부 관계자 및 사이버 리더가 참여하여 혁신적이고 효과적인 전략을 탐색하고 100여 개국에서 온 35,000명 이상의 방문객이 3일간 행사에 참석 ✓ 또한 GISEC Global 2023은 World Cyber Championship, Bug Bounty, Women in Cybersecurity, CISO Circle, Secret Briefing 등을 개최함
[중동] 중동 및 북아프리카 지역 전자상거래 규모 증가	▸ **Mena 지역 2022년 전자상거래 규모 370억 달러** ✓ 중동 및 북아프리카의 전자상거래 시장은 디지털 및 인터넷의 사용 확대에 따라 2022년에 약 370억 달러에 달했다고 EZDubai가 발표 ✓ 이는 2021년 317억 달러보다 16% 높은 수치이며, 연평균 11%의 성장률로 2026년까지 약 570억 달러에 이를 것으로 전망된다고 함 ✓ 이러한 성장은 디지털 결제 플랫폼 및 온라인 식료품 쇼핑의 인기와 기술 발전에 힘입어 인터넷 사용의 지속적인 증가에 따른 것이며 Mena 국가의 인프라와 지원 정책, 경제적 안정성, 기술 투자가 이 지역의 강력한 디지털 환경 개발을 주도한 것으로 연구는 보고하고 있음 ✓ 사우디아라비아와 UAE, 이스라엘이 전체 전자상거래 시장의 72% 이상을 차지했으며, 이들 국가의 성장은 기술의 진보, 높은 인터넷 사용률 및 강력한 정부 재정에 기인한다고 함
[중동] 중동 및 아프리카 사이버보안 시장 규모	▸ **중동 및 아프리카 사이버보안 시장 362억 달러** ✓ MarketsandMarkets의 새로운 보고서에 따르면 중동 및 아프리카 사이버 보안 시장은 2028년까지 362억 달러에 도달 할 것으로 전망 ✓ 사이버 공격의 증가, 디지털 환경의 변화, 중동 및 아프리카 전역의 온라인 비즈니스 촉진 등이 주요원인 ✓ 중동은 빠르게 성장하는 경제와 첨단 기술 인프라를 갖춘 많은 국가들이 있고 전 세계 사이버 범죄자의 주요 표적이 되고 있어 이 지역은 해킹 시도, 데이터 유출, 맬웨어 공격 및 랜섬웨어 공격을 포함한 다양한 공격에 직면해 있어 이에 대비한 더 많은 투자가 이루어지고 있다고 함 ✓ 보안 정보 및 이벤트 관리(SIEM, Security Information & Event Management) 시스템이 로그 관리 기술과 함께 2023년 이후 소프트웨어 시장 점유율이 가장 클 것으로 예상

이 슈	주 요 내 용 및 시 사 점
	▶ **시사점** ✓ 중동 및 아프리카 지역이 디지털 전환을 이루면서 전자상거래의 증가와 더불어 사이버 보안시장도 증가하여 있으며 코로나 이후 신기술과 정책을 모색하는 컨퍼런스 등이 활성화되고 있음