Research Insights

–

코로나19 사이버 전쟁: 비즈니스를 보호할 방법

대유행병을 기회로 삼아 속도를 내는 공격자들 – 즉각적인 대응을 위한 단계별 보안 가이드

IBM 기업가치 연구소

IBM

IBM의 역할

사이버 보안 문제 또는 사고를 겪고 있다면 X-Force IRIS에 연락하여 도움을 받으실 수 있습니다.
미국 핫라인 1-888-241-9812
글로벌 핫라인 (+001) 312-212-8034

추가 정보:
https://www.ibm.com/security/covid-19

Wendi Whitmore,
Gerald Parham

핵심 요점

코로나19와 사이버 전쟁

전 세계가 코로나19(COVID-19)에 맞서 분투하고 있는 가운데 사이버 범죄자들은 이러한 위기를 절호의 기회로 생각합니다. IBM X-Force는 지난 2월 이후 코로나바이러스를 주제로 한 스팸이 4,300% 증가했음을 확인했습니다. *해야 할 일: 발생 가능성이 높은 위협을 모델링하는 시뮬레이션을 당장 수행하여 모든 취약점을 최소화합니다.*

혼돈의 상황에서 즉각적인 대응

평상시에 준비가 부실했던 기업은 완전히 무방비 상태로 위기를 맞이했습니다. 실제로 한 2019년 보고서에 따르면, 조직 전반에 일관성 있게 적용할 사고 대응 계획이 없는 기업이 76%에 달했습니다.[1] *해야 할 일: 사이버 보안 사고 대응 계획(Cybersecurity Incident Response Plan, CSIRP)을 작성하거나 업데이트합니다.*

대혼란을 극복하기 위한 관리

위기가 닥치면, 비즈니스 연속성(business continuity) 계획이 중요한 전략적 자산이 됩니다. 준비 안 된 기업도 그 영향을 최소화하기 위한 조치에 나서고, 그러한 경험을 미래의 위기 대응 계획에 활용할 수 있습니다. *해야 할 일: 관찰, 방향 설정, 결정, 그리고 행동으로 이어지는 주기를 빠른 속도로 진행합니다.*

극한 상황을 경험하며 얻은 교훈

지난 몇 주간 공격자들이 코로나19 유행병을 기회로 삼으면서 사이버 보안 위협이 가파르게 증가했습니다. 각 기업에서 새로운 시급한 과제, 즉 직원의 안전, 재정 건전성, 운영 및 공급망의 레질리언스 등에 집중하는 가운데, 사이버 보안에 대한 관심이 상대적으로 줄면서 위험이 가중되고 있습니다.

위기 상황에서는 즉각적인 결정이 주를 이루므로, 데이터를 유출하고 비즈니스 운영을 방해할 기회가 늘어납니다. 그 잠재적 영향 때문에 위험이 더욱 증가합니다. 예를 들어, 분산 서비스 거부(distributed denial-of-service, DDoS) 공격이 발생하면, 이미 용량 과부하 상태에 있는 운영 조직은 즉시 추가 용량 확보가 가능한 곳보다 훨씬 더 큰 피해를 입을 수 있습니다.

본 보고서에서는 보안 리더가 현재와 같은 환경에서 일어날, 각기 다르고 영향력이 큰 사건을 제대로 관리하고, 예기치 않은 다른 시나리오에도 대비하기 위해 반드시 해야 할 조치를 소개합니다. 사이버 보안 위기 상황이 되면, 다음 3단계 라이프사이클을 거치게 됩니다.

- 계획 및 탐지
- 즉각적인 대응 및 위협 제거
- 복구

일단 리더는 현재 이 라이프사이클의 어느 단계에 있는지 확인하고, 그에 따라 필요한 조치의 우선 순위를 정해야 합니다. 이를 위한 길잡이로, IBM은 각 단계에서 해야 할 일에 대한 권장안을 마련했습니다. 특히 지금과 같은 대유행병 상황에서는 대응 및 위협 제거에 각별히 관심을 기울여야 합니다. IBM은 보안관제 센터(security operations center, SOC) 및 사이버 레인지(cyber range, 보안 기능을 테스트하는 가상 환경)에서 사고 대응 훈련을 수행한 경험을 통해 레질리언스가 뛰어난 기업일수록 3가지 영역에서 두각을 나타낸다는 사실을 확인했습니다. 그 3가지 영역은 바로 체계적인 리소스 관리 및 배포, 정기적인 커뮤니케이션, 공동 대응입니다.

50+

코로나19를 주제로 한 각종 공격 캠페인에서 배포한 고유 악성코드의 수[2]

4곳 중 1곳

사고 대응 계획이 없는 기업[3]

#1

사고 대응(IR) 팀과 사고 대응 계획 테스트를 연계하여 활용함으로써 다른 보안 위협 제거 프로세스보다 훨씬 더 큰 비용 절감 효과를 거둘 수 있습니다.[4]

코로나19가 사이버 보안 환경에 미치는 영향

2020년 들어 전 세계의 거의 모든 기업이 급격한 비즈니스 변화를 겪었습니다. 코로나19 감염 사례 및 전파 속도가 일부 지역에서는 증가하고 다른 지역에서는 주춤하는 가운데, 운영 환경이 매일, 때로는 매시간 변화하고 있습니다. 그 파급 효과도 전례 없는 수준입니다.

기회를 노리는 공격자들

이 질병이 전 세계로 확산된 2월 이후 IBM X-Force는 코로나바이러스를 주제로 한 스팸이 4,300% 증가했음을 확인했습니다. 사이버 범죄자들이 코로나바이러스 발생을 비즈니스 기회로 삼으면서 바이러스를 주제로 한 악성코드 자산이 다크 웹에서 팔리고 있으며, 심지어 바이러스와 관련된 할인 코드까지 등장했습니다.[5] 관련 도메인도 빠르게 생겨나고 있는데, 코로나19 관련 도메인은 같은 기간에 등록된 다른 도메인에 비해 악성일 가능성이 50% 더 높습니다.[6]

무수히 많은 피싱 사기가 등장했습니다. 예를 들어, IBM X-Force Exchange에서 추적 중인 한 스팸 이메일은 미국 중소기업청에서 지원하는 대출을 받으려는 소상공인을 표적으로 삼습니다. 이 이메일의 첨부 파일을 실행하면, 대출과 상관없는 RAT(Remote Access Trojan)가 설치됩니다. 또 다른 대규모 스팸 캠페인에서는 비트코인으로 몸값을 지불하지 않으면 수신자와 그 가족을 코로나19에 감염시키겠다고 위협합니다.[7]

합법적인 보건 기관과 관계 있는 것처럼 꾸미는 스캠도 많습니다. 한 이메일 피싱 공격은 세계 보건 기구(World Health Organization, WHO) 사무총장이 보낸 것처럼 위장합니다. 첨부 문서를 실행하면 설치되는 Agent Tesla 악성코드 변종은 키로거(keylogger)의 역할을 하면서 정보를 훔쳐냅니다.[8] 더 간단한 공격의 예로, 미국 질병 통제 예방 센터(US Centers for Disease Control and Prevention, CDC)를 미끼로 활용하는 것도 있습니다.[9] 각종 위협 행위자 및 코로나19 익스플로잇을 취합하는 IBM X-Force 코로나19 보안 공고에 확인한 사례도 수백 건에 달합니다.[10]

보고서에 따르면, 국가 주도형 공격자가 이 질병 확산을 틈타 미국 공중 보건 기관, 특히 미국 보건복지부를 공격할 가능성이 있습니다.[11] 미상원 정보 위원회 소속의 Ben Sasse도 이렇게 말합니다. "바로 21세기형 분쟁의 현실입니다. 사이버 공격은 쓰러진 상대방을 완전히 격파하는 데 쓰이는 대량 살상 무기라 할 수 있습니다."[12]

인사이트: 대중의 신뢰를 무너뜨리는 사이버 범죄

사이버 범죄는 질병의 대유행 과정에서 증폭되는 공포, 불안, 불확실성, 정서를 공격자가 이용할 수 있을 때 성공합니다. 설상가상으로, 개개인의 관심사, 개인과 기업의 생존 문제 등에서도 예측 불가한 혼란이 전개됩니다. 세계 경제 포럼(World Economic Forum)의 공고에서도 지적했듯이, 사회가 디지털 인프라에 더 많이 의존할수록 장애 비용(cost of failure)이 상승합니다.[13] 이 공중 보건을 위협하는 유행병은 사회적 비용과 경제적 비용을 모두 발생시키면서 개개인에게 유례 없는 지대한 영향을 미치고 있습니다. HVA(high-value asset)는 공격에 특히 취약합니다. 미국 사이버 보안 및 인프라 보안청(US Cybersecurity and Infrastructure Security Agency, CISA)에서 “매우 중요하기 때문에 유실되거나 손상되면 기업의 사명 또는 비즈니스 수행 능력에 큰 타격을 주는 정보 또는 시스템”이라고 정의한 HVA는 어떤 기업에 대한 대중의 신뢰를 무너뜨리려는 사이버 범죄자에게 더없이 매력적입니다.[14]

원격 근무의 새로운 위험성

원격 근무 체제로 빠르게 전환한 결과, 사이버 범죄자가 노릴 만한 새로운 허점도 나타났습니다. 2020년 4월 첫주에 발행된 *뉴욕 타임즈(The New York Times)*에 따르면, 미국에서 강제적으로 자택에 머물러야 하는 사람의 수가 3억 1,600만 명에 달합니다.[15] 전 세계적으로는 그 몇 배에 달할 것입니다. 인도에서도 자가격리 지침의 대상이 13억 명으로 확대되었습니다.[16]

이 자가격리자의 상당수가 재택 근무 중입니다. 하지만 근무 장소가 바뀐 직원의 상당수는 디지털 안전을 지키기 위한 보안 장비 또는 프로토콜이 없는 상태입니다. 새롭게 원격 근무하는 직원이 개인용 디바이스를 통해 기업 네트워크에 액세스할 때 해커는 Wi-Fi 구성 및 VPN 연결을 탐색하여 보안 취약점을 찾아냅니다. 업무 및 개인적 용도로 클라우드 기반의 생산성 플랫폼을 이용하는 사람이 늘자, 공격자는 라이브 미팅을 해킹하고 교란하는 등 현재의 상황을 십분 활용하는 작전을 시작했습니다.[17]

준비 안 된 것은 직원만이 아닙니다. 기업도 마찬가지입니다. 최근 Threatpost의 온라인 설문조사에서는 해당 기업에서 원격 근무 모델을 비교적 최근에 도입했다는 응답자가 70%에 달했습니다. 그리고 40%는 원격 근무를 지원하면서 사이버 공격이 증가하고 있다고 밝혔습니다.[18] 미국의 Mark Warner 상원의원도 이메일에서 이렇게 지적했습니다. "연방 정부가 사상 초유의 텔레워크 시범 운용을 준비하는 과정에서 공격자가 행동에 나서 중요 정부 서비스를 교란시킬 가능성도 커지고 있습니다.”[19]

이 대유행병 상황에서 혼란이 계속될 가능성이 높은 만큼, 위기 대응 책임자는 계속 경계를 늦추지 않고 애자일 조직 환경을 유지해야 합니다.

레질리언스가 뛰어난 기업은 효과적으로 리소스를 취합하여 운용하고, 효율적으로 의사소통하며, 공동의 대응을 수행합니다.

빠른 의사결정의 중요성

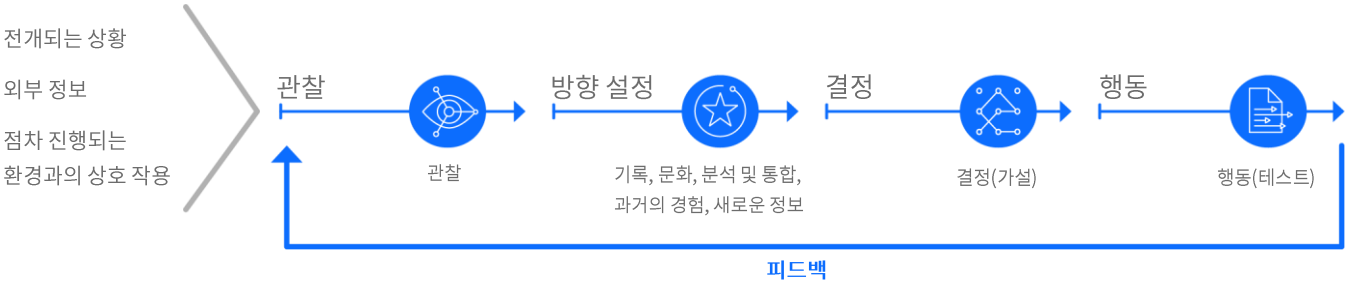
위기 상황에서는 경영진과 보안 팀이 가용 정보를 필터링하여 빠르게, 최상의 결정을 내려야 합니다. 원래 군 전략가들이 개발한 원칙, 즉 "OODA(observe, orient, decide, act)" 루프와 같은 전술 작전 기법을 도입하여 효과를 거두는 기업도 있습니다.[20]

OODA 루프는 반복 실행을 강조합니다(그림 1 참조). 어떤 위협 제거 상황에서도 이 루프를 더 빠르게 진행한다면 우위를 확보할 수 있습니다. 대응 속도를 높이면서 더 광범위한 팀과 연계하고 협업할 수 있습니다. 꼭 최종 결정이 될 필요는 없습니다. 아무런 조치도 하지 않는 것보다는 사소한 실수를 하더라도 행동하는 것이 나은 법입니다.

—

그림 1

OODA(Observe, Orient, Decide, Act) 루프



출처: "OODA loop." Wikipedia, 2020년 4월 1일. https://en.wikipedia.org/wiki/OODA_loop

사고 대응 계획 수립

대부분의 기업이 중대한 사이버 보안 사고를 처리할 준비가 제대로 되어 있지 않습니다. 게다가 코로나19와 같은 전 세계적인 위기 상황에서는 훨씬 더 심각해집니다. Ponemon Institute의 최근 연구에 따르면, 조직 전반에 일관성 있게 적용할 사고 대응 계획이 없는 기업이 76%에 달했습니다. 기업 4곳 중 1곳이 어떤 형태의 CSIRP(Cybersecurity Incident Response Plan)도 갖추지 못했다고 밝혔습니다.[21]

효과적인 CSIRP라면, 모든 팀의 거버넌스 및 커뮤니케이션 절차를 개괄적으로 정리합니다("인사이트: CSIRP 집중 해부" 참조). 또한 대응 모델을 정의하고, 조직 전 범위의 위기 대응 역할 및 책임을 상세히 규정합니다. 여기에는 전략, 기술, 운영, 커뮤니티/정부 관계도 포함됩니다. CSIRP가 아직 없는 기업은 서둘러 마련해야 합니다. 코로나19가 확산되기 전부터 세계 전역에서 침해 사고 고지에 관한 법률 및 규제가 강화되고 있던 만큼, 비즈니스 연속성 계획이 장기적으로 중요한 전략 기능이며, 이 계획을 통해 여러 예기치 못한 비상 사태에 대비할 수 있습니다.

하지만 CSIRP가 있는 기업도 코로나19와 관련된 위험에 맞서 이를 강화하는 노력을 기울여야 합니다. 위기 관리 계획은 위협의 성격 및 범위, 조직의 유형 및 규모 그리고 정보 공개, 개인정보보호, 데이터 지역성과 관련된 규제 요건의 차이에 따라 달라집니다. 더 많이 학습한 기업은 신속하게 CSIRP를 수정하면서 학습한 내용을 적용할 수 있습니다.

인사이트: CSIRP 집중 해부

일반적으로 사이버 보안 사고 대응 계획(CSIRP)은 다음 정보로 구성됩니다.

- 위기 상황을 파악하고 분류하는 방법
- 사내외 팀원의 역할 및 책임 – 의사결정 권한 및 에스컬레이션 절차를 요약하는 계층형 보기 포함
- 사내외 이해 관계자와의 의사소통을 위한 위기 커뮤니케이션 계획
- 기업의 HVA 및 미션 크리티컬 기능의 인벤토리 – 이를 활용하기 위한 중요 지원 서비스 포함
- 위 항목과 관련된 규제 및 공개 요건
- 보조 운영 지원 기능의 인벤토리 - 위협 제거 서비스 및 커뮤니티/CERT(computer emergency response/readiness team), 연방 법 집행 기관, 기타 관계자 그룹과의 보안 위협 인텔리전스 공유 포함

아무런 조치도 하지 않는 것보다는 사소한 실수를 하더라도 행동하는 것이 나은 법입니다.

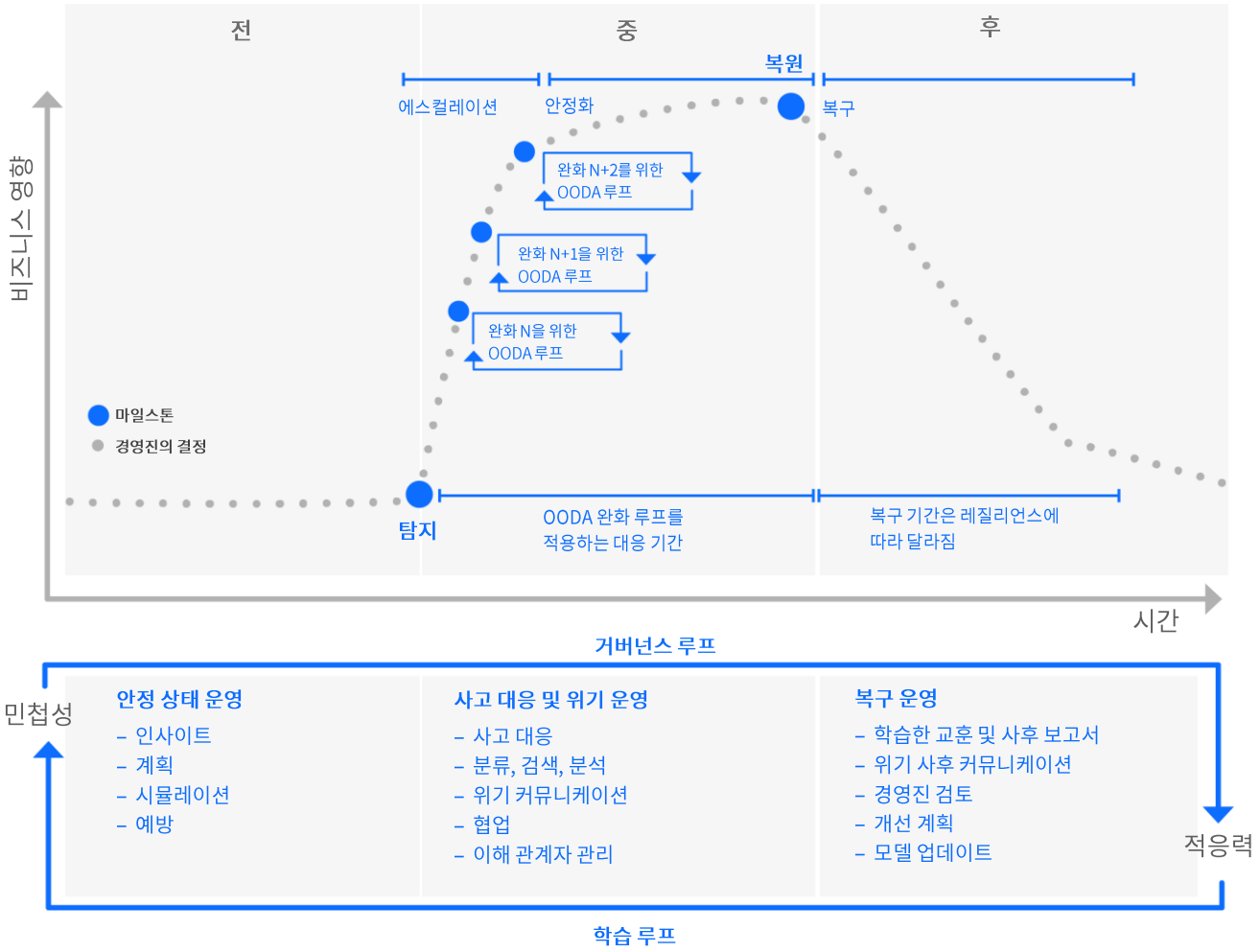
위기 라이프사이클, 1단계: 안정 상태/계획

코로나19 위기가 확산되는 가운데 아직 사이버 위협을 겪지 않은 기업이라면 대비할 시간이 있습니다. 이 시간을 현명하게 사용해야 합니다. (그림 2 참조)

무엇보다도 CSIRP가 없는 기업은 서둘러 마련해야 합니다. 계획 단계를 이미 마친 리더라면, 이제 코로나19 보안 실태에 따라 CSIRP에 허점이 없는지 평가할 차례입니다. 코로나19와 같이 "블랙 스완" 현상이 장기적인 현실로 자리잡더라도 선택할 수 있는 옵션은 있습니다.[22] 이러한 옵션을 발전시킬 방법을 모색하고 더 현명한 결정을 내리기 위한 시간을 확보하는 것이 관건입니다.

그림 2

위기 라이프사이클



기업의 재해 대응 능력은 시뮬레이션을 통해 발전시킬 수 있습니다. 현실적인 실전 경험을 대체할 수는 없지만, 훈련 및 반복 중심의 시뮬레이션은 위험 관리 및 위험 완화 모델의 허점을 찾아내는 데 효과적입니다. 팀이 더 많은 시뮬레이션을 하면 무엇을 예상해야 하는지 그리고 실제 보안 사건이 벌어지면 어떻게 대응할지를 더 잘 알게 됩니다. 팀은 실시간으로 전개되는 변수 및 종속성을 확인하면서 대응을 모델링하고 계속 업그레이드할 수 있습니다.

위험 관리 정의

사이버 레질리언스는 기업이 사이버 공격을 예방하고 대응하며 그로부터 복구하는 능력뿐만 아니라 사내외 운영의 무결성을 유지하는 능력까지를 의미합니다. 특히 우려할 3대 요소는 위협 요소, 취약점, 위험입니다.

- *위협 요소:* 의도적이든 우연이든 어떤 취약점을 악용하면서 정보 또는 운영 자산을 차지하거나 손상시키거나 파괴시키는 모든 것. 이는 개별적인 전술 또는 사건에 해당합니다.
- *취약점:* 어떤 위협 요소가 어떤 자산에 무단 접근하기 위해 악용할 수 있는 보안 프로그램의 약점 또는 허점.
- *위험:* 어떤 위협 요소가 어떤 취약점을 노린 결과 발생할 수 있는 손실, 손상, 파괴 가능성.[23]

특히 코로나19가 유행 중인 시기에는 위험이 역동적이고 새롭게 발생하며 예측 불가하고, 대개는 상호 의존 관계에 있다는 점 때문에 어려움이 가중됩니다. 위험 관리란 각종 위협 요소를 파악하고, 발생 확률과 연계하여 운영에 미칠 영향의 정도를 모델링하는 것입니다. 이런 까닭에 사이버 대응에는 사이버 보안, 기술, 운영 팀의 협업, 즉 범부서 (그리고 점차 범조직) 차원의 활동이 필요합니다.

위험이 현실화되면, 각 팀은 계획 및 모델링 모드에서 사고 대응, 재해 복구, 비즈니스 연속성 모드로 운영을 전환해야 합니다. 무엇보다도, 계획/시뮬레이션 프로세스가 실행/대응 프로세스와 동일해야 합니다. 협업을 통해 신속하게 의사결정하는 능력이 성패를 가를 때가 많습니다.

1단계: 해야 할 일

여러 업무 영역 연계, 플레이북 실행 및 업그레이드

1. 계획을 세우고 팀을 조직합니다. CSIRP를 만듭니다. 이 계획은 현재 운영 환경을 반영하여 정기적으로 업데이트합니다. 위기 알림 대상자 명단을 검증하고 테스트하여 팀을 정비합니다. 반년 또는 분기 단위로 계획을 업데이트하고 위기 대응 훈련을 실시하는 방안을 고려합니다. 특히 인사 이동이 빈번한 대규모 조직일수록 이러한 조치가 필요합니다.

2. 의사결정을 애자일 모드로 전환합니다. 이전에 개발하여 테스트한 프로세스 및 절차가 있다면, 대응 계획을 이행하는 주요 이해 관계자의 신속한 의사결정을 지원해야 합니다. 핵심 리더는 오래 걸리는 승인 프로세스를 거치지 않고 중요한 결정을 내릴 권한이 있어야 합니다.

3. 종속성을 없애고, 전방향으로 가시성을 확대합니다. 자주 간과되는 위험 영역 중 하나가 공급망 가용성 및 무결성입니다. 마찰을 해소하고 의사결정 속도를 높이며 공급자 상호 의존 관계를 유지하기 위해 투명성의 메커니즘을 적용합니다. 지역별 또는 공급자별 구매 종속 관계를 파악하고, 중단 없는 비즈니스 운영을 위해 대체 공급원을 찾습니다. 제공자/공급자 계약에서 불가항력(피할 수 없는 대형 사고 포함) 관련 조항을 재검토합니다. 공급망 네트워크에 제4자 및 "제n자" 관련 위험이 없는지 점검합니다.

4. 현실적인 계획을 세웁니다. 탁상 훈련 및 보안 침해 시뮬레이션은 사이버 위기 관리 계획의 주요 기능별로 프로세스 및 절차를 검증하는 효과적인 방법입니다. 정기적으로 전체 규모의 시뮬레이션 연습을 통해 팀, 경영진, 커뮤니케이션에 대한 스트레스 테스트를 진행합니다. 군사 조직의 1차 대응팀처럼 효과적으로 대처할 "근육 기억을 가진" 팀을 육성하는 것이 궁극적인 목표입니다. 위기 계획에서는 운영 중단 및 사회적 영향의 전 범위를 수용해야 합니다. 그러기 위해서는 다각도의 위기 완화 및 대응 접근법이 필요합니다.

5. 실수로부터 배웁니다. 위기 시뮬레이션에서 발생한 실패가 실제 위기 상황의 실패보다 더 유익하고 경제적입니다. 시스템상의 의존성, 낡은 가설, 의사결정 편향으로 인해 장애 유형(failure mode)별로 어떻게 악화되는지를 확인하세요. 모든 훈련에서 예기치 못한 요소를 포함시켜 표준 관행 및 위기 거버넌스에 팀의 협업 문제 해결 능력 및 독창성을 균형적으로 접목합니다.

위기 라이프사이클, 2단계: 사고 대응

철저한 계획 및 대비에도 불구하고 위기는 그 속성상 예기치 않게 불어닥칩니다. 코로나19 대유행처럼 무차별로 조직을 강타하면 시스템 차원의 장애가 발생하기 마련입니다. 시스템 차원의 위기 상황에서는 일상적인 운영 기능이 중요 인프라의 필수 조건으로 분류되고, 대규모의 조정 작업을 거쳐야 운영이 안정화될 수 있습니다.

실제 위기가 발생하면, 시뮬레이션 훈련을 통해 대응 계획을 업데이트하고 역량을 강화했던 팀이 훨씬 더 유리합니다. 팀이 무엇을 해야 하는지를 알고 있으므로, 리더는 상황의 추이를 관찰할 수 있습니다. 그런 다음 필요한 시점에 결정을 내리고 방향을 수정하여 직원, 고객, 기타 이해 관계자의 안전을 보장하고, 데이터 무결성을 지키며, 해당 위기를 최소화하는 방향으로 각종 사건에 대응할 수 있습니다.

무차별적인 위기 상황에서 심각한 사회 혼란이 일어날 경우, 기업은 운영 리소스를 새로운 방식으로 활용하면서 도움을 제공하고 신뢰를 회복해야 합니다. 올바른 대응 계획이 있으면 다양한 변수를 고려할 수 있으므로, 리더가 회사의 영업권, 무결성, 신뢰를 강화할 대응 전략을 선택하는 것이 가능합니다.

위기 운영

위기를 극복하려면 거버넌스와 독창성의 절묘한 균형이 필요합니다. 중요 커뮤니케이션을 위한 거버넌스 지침을 마련함으로써 더 창의적인 문제 해결 및 협업의 기반을 조성하여 더 까다로운 위기도 완화할 수 있습니다. 기술적인 문제로 보이더라도, 그 해결 방안에는 인간의 감수성 및 팀워크가 개입되기 마련입니다.

보안 침해 또는 사이버 공격이 발생하면, 경영진은 신속하게 고객 및 이해 관계자에게 총력을 다해 문제를 해결할 것임을 알려 신뢰감을 주어야 합니다. 최고 경영진의 입장에서 이처럼 빠르고 직관적인 대응 능력이 저절로 생기는 경우는 드뭅니다. 보안 침해에 대한 기술적 해결 방법은 알고 있더라도 인간적 요소를 처리할 준비가 되지 않은 경우가 많습니다.

플레이북 및 시뮬레이션은 위기가 진행되는 과정에서 보안 팀부터 커뮤니케이션 및 PR 전문가 그리고 CEO까지 모든 관계자가 각자의 역할을 이해하고, 팀의 선제적 문제 해결에 필요한 하드 스킬과 소프트 스킬의 최적의 조합을 제대로 구사하며 대응하는 데 큰 도움이 됩니다.

2단계: 해야 할 일:

플레이북 실행, 적응, 협업

1. **완벽할 수 없음을 인정하고 현재에 충실합니다.** 분류가 필요하고 최초의 성과가 미흡할 수 있음을 인정합니다. “관찰, 방향 설정, 결정, 행동”의 주기를 빠르게 진행하여 선제적으로 대처합니다. 복잡한 문제는 더 작은 구성요소로 나눕니다.

2. **인지 부하를 최소화합니다.** 표준화된 용어 및 커뮤니케이션 프로토콜을 적용하여 팀원들의 인식을 동기화함으로써 검색 및 평가 속도를 높입니다. 정보를 필터링하고, 변수는 최대한 간단히, 직접적으로 나타냅니다. 시각적 요소를 활용하여 주요 관계 및 종속성을 나타냅니다.

3. **솔선수범합니다.** 리더는 소프트 스킬과 하드 스킬을 복합적으로 구사합니다. 기술적 능력뿐만 아니라 심사숙고하고 공감하는 태도를 보여줍니다. 상황의 변화에 따라 행동과 분석의 적절한 조합을 모델링합니다. 팀원들이 사실과 의견의 차이점을 분명히 인식하게 합니다.

4. **영웅적 행위 또는 자기 희생보다 팀워크에 우선순위를 둡니다.** 팀의 강점을 상세히 조사하고, 팀의 다양성을 십분 활용합니다. 관심도 및 역량에 따라 책임을 부여합니다. 파트너도 핵심 팀원으로 받아들여 권리와 책임을 부여합니다. 거시적 관점에서 압도하기보다는 격려하고 영감을 줍니다.

5. **특히 고위직 리더 및 이해 관계자와 정직하고 투명하게 소통합니다.** 비즈니스에 대한 위협을 구체적인 용어로 정의하는 방법을 익힙니다. 어떤 지표가 발전을 의미할까요? 전문 인력, 예산, 시간을 더 많이 투자하면 달라질까요? 이번 위기는 다른 위기와 비교하면 얼마나 비슷한가요(그리고 다른가요)? 어떤 변수 때문에 상황이 악화되거나 향상되고 있나요? 어떤 결정을 에스컬레이션해야 할 시점을 알고, 여러 선택 사항 및 예상되는 결과를 준비합니다.

위기 라이프사이클, 3단계: 복구 및 개선

어떤 보안 전문가들은 코로나19 대유행에서 영감을 얻어 이처럼 대규모로 사회적 혼란을 야기할 미래의 사이버 공격이 나타날 수도 있다고 생각합니다.[24] Brian Finch도 The Hill에 실은 사설에서 이렇게 말합니다. “워싱턴의 사이버 전략가들은 코로나19의 경제적 피해를 최소화하는 데 성공한 방법을 면밀하게 연구해야 합니다. 그러한 노력을 통해 피할 수 없는 사이버 팬데믹이 일어나더라도 불필요하게 혼란을 야기하는 대책 및 임시방편이 쏟아지는 것을 막을 수 있습니다.”[25]

코로나19가 전 세계에 경종을 울린 것은 분명합니다. 모든 대격변이 그러하듯 경험을 통해 얻은 교훈이 향후 더 나은 대안을 마련하는 데 도움이 될 수 있습니다. 한 가지는 분명합니다. 소통하고 조정하며 협업하는 능력이 명령하고 통제하는 능력 못지않게 성공의 비결이라는 것입니다.

보안 리더는 예방 및 차단, 사고 대응 훈련, 시뮬레이션의 조합을 통해 위기의 순간을 극복할 수 있다는 확신, 그리고 무결성의 운영에서 얻는 신념을 강화할 수 있습니다. 사이버 보안 회사, BlackCloak의 CEO인 Chris Pierson는 이렇게 말합니다. “사이버 범죄자는 전염병이 전 세계에 유행하는 이 시기에도 쉬지 않습니다. 물론 이에 맞서는 방어 전문가 및 그들의 협력업체도 마찬가지입니다. 그러므로 전망은 매우 밝다고 생각합니다.”[26]

3단계: 해야 할 일

기업의 레질리언스 및 적응력을 한층 더 강화하기 위해 새로운 기능에 투자

1. **보안 텔레메트리 및 분석을 구현합니다.** 조기 탐지 및 대응이 가능하려면 먼저 자동화된 데이터 수집 기능이 필요합니다. 첨단 텔레메트리 및 로그 파일 캡처 솔루션을 활용하여 사후에도 공격 경로를 모델링하고 시그니처를 생성하며 보안 침해를 재현할 수 있습니다.

2. **보안 자동화 기능을 개발합니다.** 보안 자동화를 실현하면, 전문가가 심층 분석이 필요한 위협에 집중할 수 있습니다. Ponemon의 연구에 따르면, 자동화에 투자하면 기대한 효과를 거둘 수 있습니다. 보안 자동화를 구축하지 않은 기업에서 데이터 유출 사고가 발생할 경우, 완벽하게 자동화를 구현한 조직에 비해 95% 더 많은 비용을 부담합니다(자동화를 구현하지 않은 경우 516만 달러, 완벽하게 자동화를 구현한 경우 265만 달러).[27]

3. **보안 위협 인텔리전스를 활용하고 참여합니다.** 클라우드 기반 보안 서비스는 단일 조직보다 훨씬 더 큰 규모의 운영 환경을 대상으로 트래픽을 모니터링합니다. 보안 위협 인텔리전스에 참여하여 데이터를 제공함으로써 모든 기업의 사이버 레질리언스를 강화할 뿐만 아니라, 위협 인텔리전스 인사이트를 활용하여 더 빨리 위협을 탐지하고 대응할 수 있습니다.[28]

4. **협업 및 지속적인 학습에 우선순위를 둡니다.** 사이버 레질리언스를 갖춘 기업은 탐색, 학습, 적응, 반복의 주기를 반복합니다. 위기 상황에서 효과적으로 보안 위협을 제거하려면, 개개인이 제대로 협업하면서 복잡하고 까다로운 문제 해결에 참여해야 합니다.[29]

5. **보안에 대한 인식을 제고합니다.** 사이버 레질리언스를 갖춘 기업은 보안을 전사적 차원의 전략적 역량으로 간주하면서 우선순위에 둡니다. 이와 같이 보안을 우선순위에 두지 않는 곳이 많습니다. IBM이 Ponemon과 함께 진행한 2019년 사이버 레질리언스 연구에서 회사의 사이버 레질리언스를 우수하다고 평가한 응답자는 25%에 불과했습니다. 그리고 사이버 공격 이후 복구하는 능력을 우수하다고 평가한 응답도 31%밖에 되지 않았습니다.[30]

저자 소개

Wendi Whitmore

IBM Security, X-Force 위협 인텔리전스 부사장
wwhitmor@us.ibm.com
linkedin.com/in/wendiwhitmore2
@wendiwhitmore

IBM X-Force 위협 인텔리전스 부사장인 Wendi Whitmore는 사이버 보안 분야의 권위자로 인정받고 있습니다. 그녀는 15년 넘게 거의 모든 업종 및 지역의 고객과 함께 사고 대응, 선제적/전략적 정보 보안 서비스, 인텔리전스, 데이터 유출 사고 조사 활동을 수행하면서 풍부한 경험을 쌓았습니다.

Gerald Parham

IBM 기업가치 연구소, 보안 및 CIO 리서치 리더 gparham@us.ibm.com
linkedin.com/in/gerryparham/

Gerald Parham은 IBM 기업가치 연구소에서 보안 및 CIO 담당 글로벌 리서치 리더를 맡고 있습니다. Gerald의 주요 연구 관심 분야는 사이버 라이프사이클 및 사이버 밸류 체인, 특히 전략, 위험, 보안관제, ID, 개인정보 보호, 신뢰의 상관성입니다. 그는 20년 넘게 경영진 리더십, 혁신, 지적 자산 개발 분야에서 일해온 베테랑입니다.

변화하는 세상에서 함께할 최고의 파트너

IBM은 고객과 긴밀하게 협업하면서 비즈니스 인사이트, 전문 연구와 기술을 접목시켜 시시각각 변화하는 오늘날의 환경에서 고객이 차별화된 이점을 확보할 수 있도록 지원합니다.

IBM 기업가치 연구소

IBM Services 산하 IBM 기업가치 연구소에서는 공공 및 민간 분야의 주요 쟁점에 대해 사실에 기반한 전략적 인사이트를 개발하여 기업의 최고경영진에게 제공하고 있습니다.

추가 정보

이번 IBM 기업가치 연구소의 연구 조사에 대한 자세한 내용은 iibv@us.ibm.com에 문의하세요. 트위터에서 @IBMIBV를 팔로우하실 수 있습니다. IBM 기업가치 연구소의 전체 연구 카탈로그가 필요하거나 월간 뉴스레터를 구독하려면 ibm.com/ibv를 방문하세요.

관련 보고서

“COVID-19 Action Guide”
ibm.co/covid-19-action-guide

“A CIO’s guide to extreme challenges”
ibm.co/cio-guide-challenges

“How CISOs can secure a strategic partnership”
ibm.com/thought-leadership/institute-business-value/ report/ciso-strategic-partnership

참고 및 출처

1 “The 2019 Cyber Resilient Organization.” Ponemon Institute, IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

2 XF-IRIS 내부 데이터 분석. 코로나19와 관련된 추가 데이터 인사이트: https://exchange.xforce.ibmcloud.com/collection/Threat-Actors-Capitalizing-on- COVID-19-f812020e3eddbd09a0294969721643fe

3 “The 2019 Cyber Resilient Organization.” Ponemon Institute, IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

4 “2019 Cost of Data Breach Study: Global Analysis.” Ponemon Institute. IBM의 의뢰를 받아 Ponemon Institute LLC가 독립적으로 수행한 벤치마크 연구. 2019. https://www.ibm.com/ downloads/cas/ZBZLY7KL

5 Whitney, Lance. “Cybercriminals exploiting coronavirus outbreak with virus-themed sales on the dark web.” TechRepublic. 2020년 3월 19일. https://www.techrepublic.com/article/cybercriminals-exploiting- coronavirus-outbreak-with-virus-themed-sales-on- the-dark-web/

6 “Update: Coronavirus-themed domains 50% more likely to be malicious than other domains.” Check Point 블로그, 2020년 3월 27일. https://blog.checkpoint.com/2020/03/05/update-coronavirus- themed-domains-50-more-likely-to-be-malicious- than-other-domains/

7 “U.S Small Business Administration Spoofed In Remcos RAT Campaign.” IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Small-Businesses-Seeking-Disaster-Assistance-Targeted-By-Remcos-Infostealer-e8b9f4f5e9d8c98f51e2ee09ac632ef8; “Holding Your Health For Ransom: Extortions On The Rise.” IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Holding-Your-Health-For-Ransom-Extortions-On-The-Rise-1fc43fac1cf1b72a4245f0107da283e3

8 “Covid-19 Drug Advice From The WHO Spoofed to Distribute Agent Tesla Info-Stealer.” IBM X-Force Threat Intelligence. IBM X-Force Exchange. https://exchange.xforce.ibmcloud.com/collection/Covid-19-Drug-Advice-From-The-WHO-Disguised-As- HawkEye-Info-Stealer-2f9a23ad901ad94a86687319 32ab5826

9 Vergelis, Maria. “Coronavirus phishing.” Kaspersky Daily. 2020년 2월 7일. https://www.kaspersky.com/blog/coronavirus-phishing/32395/

10 Whitmore, Wendi. “IBM X-Force Threat Intelligence Cybersecurity Brief: Novel Coronavirus (COVID-19).” 2020년 3월 17일. https://securityintelligence.com/posts/ibm-x-force-threat-intelligence- cybersecurity-brief-novel-coronavirus-covid-19/

11 Stein, Shira, Jennifer Jacobs. “Cyber-Attack Hits U.S. Health Agency Amid Covid-19 Outbreak.” Bloomberg. 2020년 3월 16일. https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19- response

12 Miller, Maggie. “Top US health agency suffers cyberattack.” The Hill. 2020년 3월 16일. https://thehill.com/policy/cybersecurity/487756-top-us-health-agency-suffers-cyberattack-report

13 Pipikaite, Algirde, Nicholas Davis. “Why cybersecurity matters more than ever during the coronavirus pandemic.” World Economic Forum. 2020년 3월 17일. https://www.weforum.org/agenda/2020/03/coronavirus- pandemiccybersecurity/

14 “CISA Insights.” US Cybersecurity and Infrastructure Security Agency 웹사이트, 2020년 3월 29일. https://www.cisa.gov/insights

15 Mervosh, Sarah, Denise Lu, Vanessa Swales. “See Which States and Cities Have Told Residents to Stay at Home.” *The New York Times.* 2020년 3월 29일. https://www.nytimes.com/interactive/2020/us/coronavirus-stay-at-home-order.html

16 Gettleman, Jeffrey, Kai Schultz. “Modi Orders 3-Week Total Lockdown for All 1.3 Billion Indians.” *The New York Times.* 2020년 3월 24일. https://www.nytimes.com/2020/03/24/world/asia/india-coronavirus-lockdown.html

17 Miller, Maggie. “Zoom vulnerabilities draw new scrutiny amid coronavirus fallout.” The Hill. 2020년 4월 2일. https://thehill.com/policy/cybersecurity/ 490685-zoom-vulnerabilities-exposed-as-meetings- move-online

18 Seals, Tara. “Coronavirus Poll Results: Cyberattacks Ramp Up, WFH Prep Uneven.” Threatpost. 2020년 3월 19일. https://threatpost.com/coronavirus-poll-cyberattacks-work-from-home/153958/

19 “Federal employees may soon be ordered to work from home.” *The Washington Post.* 2020년 3월 13일.

20 “OODA loop.” Wikipedia, 2020년 4월 1일. https://en.wikipedia.org/wiki/OODA_loop

21 “The 2019 Cyber Resilient Organization.” Ponemon Institute, IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

22 블랙 스완(black swan) 현상은 일반적인 예상의 영역을 벗어나는 완전한 뜻밖의 극한 상황을 의미합니다. Taleb, Nassim Nicholas. “The Black Swan: The impact of the highly improbable.” 2007.

23 “Threat, vulnerability, risk—commonly mixed up terms.” Threat analysis Group 웹사이트, 2020년 4월 1일. https://www.threatanalysis. com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms/

24 Kallberg, Jan, Col. Stephen Hamilton. “What COVID-19 can teach us about cyber resilience.” Fifth Domain. 2020년 3월. https://www.fifthdomain.com/opinion/2020/03/23/what-covid-19-can-teach-us-about-cyber-resilience/

25 Finch, Brian. “Cyber planners should be carefully watching the coronavirus.” The Hill. 2020년 3월 2일. https://thehill.com/opinion/cybersecurity/485391-cyber- planners-should-be-carefully-watching-the-coronavirus

26 Ferguson, Scott. “Cybersecurity Sector Faces Reckoning After Coronavirus Hits.” BankInfoSecurity. 2020년 3월 10일. https://www.bankinfosecurity.com/ coronavirus-hits-wall-street-cyber-survive-slide-a-13913

27 “2019 Cost of Data Breach Study: Global Analysis.” Ponemon Institute. IBM의 의뢰를 받아 Ponemon Institute LLC가 독립적으로 수행한 벤치마크 연구. 2019. https://www.ibm.com/ downloads/cas/ZBZLY7KL

28 예: IBM X-Force 위협 인텔리전스 인덱스(연례 보고서). https://www.ibm.com/security/ data-breach/threat-intelligence

29 “High-Stakes Hiring: Selecting the Right Cybersecurity Talent to Keep Your Organization Safe.” IBM Smarter Workforce Institute. 2018. https://www.ibm.com/downloads/cas/X47BR759

30 “The 2019 Cyber Resilient Organization.” Ponemon Institute, IBM. 2019. https://www.ibm.com/downloads/cas/GAVGOVNV

Research Insights 소개

Research Insights에서는 공공 및 민간 분야의 주요 쟁점에 대해 사실에 기반한 전략적 인사이트를 개발하여 기업의 최고 경영진에게 제공하고 있습니다. IBM 기업가치 연구소의 주요 연구 분석 결과를 토대로 합니다. 자세한 내용은 IBM 기업가치 연구소(iibv@us.ibm.com)에 문의하세요.

IBM Corporation
New Orchard Road
Armonk, NY 10504
Produced in the United States of America
2020년 4월

이 보고서는 일반 지침으로만 제공됩니다. 세부적인 연구나 전문가 의견의 예제를 대체할 수 없습니다. IBM은 본 문서에 의존한 개인 또는 조직에 발생한 어떠한 손해에 대하여도 책임을 지지 않습니다.

44031444KRKO-01