PKI 자동화 현황

2021년 보고서

PKI 자동화 현황 보고서

PKI는 거의 모든 기술의 중심입니다. 사용자 인증 및 서명, 서버, 장치, IoT, DevOps 애플리케이션 및 서비스, 디지털 문서 서명 및 다양한 측면에서 매우 중요한 역할을 합니다.

그러나 PKI의 수동 관리가 어려워지는 순간이 곧 다가옵니다. 최근 Ponemon 연구에 따르면 기업이 관리해야 하는 PKI 인증의 개수는 매년 43%씩 증가했습니다[1]. 게다가 인증서 유효 기간의 단축 등으로 기업들은 PKI 인증서 관리의 워크로드에 압도됩니다.

기업이 이러한 문제의 처리 방법을 더 잘 이해할 수 있도록 텍사스주 댈러스에 위치한 ReRez Research는 DigiCert의 위임을 받아 전 세계 400여 곳 기업에서 PKI 관리 담당 IT 관리자를 대상으로 설문조사를 실시했습니다. 설문조사 결과는 PKI 인증서 문제에 대한 전체적인 그림을 제시하고 있으며 기업의 PKI 관리 파악 수준에 대한 통찰력을 전달합니다.

기업이 관리해야 하는
PKI 인증서 개수의 증가: **43%**

PKI 자동화란?

설문조사 응답자를 위하여 PKI 자동화는 다음과 같이 정의되었습니다:

- 기존 디지털 인증서의 검색
- 새로운 디지털 인증서의 발행
- 만료 전 디지털 인증서 갱신하기
- 필요 시 디지털 인증서 폐기
- 코드 서명의 자동화
- 고객 인증서의 등록 절차
- 신원 확인(예: 문서 서명)
- LDAP 및 거래소 진입 등 확장된 프로비저닝 활동의 자동화
- 기타 PKI 관리와 관련된 내부 활동

1 2020년 글로벌 PKI 및 IoT 트렌드 연구(Ponemon)

혼란을 야기하는 PKI의 빠른 성장

연구에 참여한 일반적인 기업들은 현재 50,000개 이상의 인증서를 관리하고 있습니다. 가장 일반적인 인증서 유형은 사용자 및 서버용 인증서이며 그 다음은 웹 서버, 모바일 장치, 이메일이었습니다. 기업들은 내부 사설 CA가 발행한 사설 인증서에 비하여 공공 인증서 또는 공공 인증 기관(CA)이 발생한 인증서를 3배 더 많이 관리합니다.

현재 기업들은 일반적으로 **50,000**개 이상의 인증서를 관리합니다.

이는 최근 몇 년간 급격하게 증가했으며 기업들이 워크로드 관리 문제를 겪고 있다는 다양한 증거가 있습니다. 실제로 2/3은 예상치 못한 인증서 만료로 인한 운영 중단을 경험했습니다. 1/4의 기업은 지난 6개월 동안 5~6회의 운영 중단을 경험했습니다.

이유는 무엇일까요? 그 이유는 워크로드의 증가에서 일부 찾아볼 수 있습니다. 거의 2/3에 가까운 기업은 인증서 관리에 소요되는 시간에 대해 상당히 우려하고 있습니다. 또 다른 문제는 가시화의 부족입니다. 37%의 기업들은 인증서 관리를 위해 3개 이상의 부서를 운영하기 때문에 혼란을 야기합니다. 일반적인 기업들은 실제로 거의 1,200개에 가까운 인증서를 관리하지 않으며 거의 절반인 47%의 기업들은 IT 팀이 인식하지 못하거나 관리하지 않는 '비인가' 인증서를 종종 발견한다고 답했습니다. 이러한 문제에 대한 명백한 솔루션은 PKI 자동화이므로 관련 기업들의 PKI 자동화 현황에 대하여 탐구했습니다.

61% 는 인증서 관리에 소요되는 시간 문제를 겪음

47% 는 비인가 인증서를 자주 만남

37% 는 인증서 관리 부서를 3개 이상 운영함

4분의1 

는 지난 6개월 동안 5~6건의 PKI 관련 운영 중단을 경험함

91%의 기업들은 PKI 자동화를 원함

설문조사 결과에 따르면 약 91%, 대부분의 기업은 최소한 PKI 자동화에 대하여 논의를 진행하고 있습니다. 단지 9%의 기업만이 PKI 자동화를 논의하지 않으며 그럴 계획이 없다고 답했습니다. 70%의 대부분의 기업은 12개월 내에 솔루션을 구현할 예정입니다. 1/4은 실제로 솔루션을 이미 구현하고 있거나 구현을 완료하는 단계에 있습니다. 그러나 구현이 쉽지는 않습니다. 기업들은 높은 자동화 비용, 복잡성, 규정 준수 문제, 변화에 저항하는 직원 및 경영진 등의 문제가 있다고 답합니다.

트렌드

기업들이 PKI 자동화를 채택하는 공통적인 이유:

1. 비인가 인증서
2. 퀀텀 컴퓨팅 이후의 준비
3. 워크로드를 기하급수적으로 증가시키는 인증서 유효 기간의 빠른 감소
4. 관리 대상 인증서 개수의 급격한 증가
5. 원격 근무 트렌드

부정적인 요소

기업의 자동화를 추진하는 보안 문제:

1. 새로운 인증서 프로비저닝의지연
2. 잘못 구성되는 인증서 경향
3. 과도한 직원 업무 부하
4. 너무 많은 비인가 인증서
5. 인증서 만료 기간을놓침
6. 필요 시 인증서 폐기의 지연 또는 실패

불이익

PKI 비자동화로 인한 부정적인 비용:

1. 규정 준수 문제
2. 보안 문제
3. 비용
4. 운영 중단
5. 고객 또는 직원의 불만

목표

PKI 자동화를 구현하는 기업의 목표:

1. 보안 개선
2. 컴플라이언스 개선
3. 더 민첩한 대응
4. 생산성 향상
5. 중단 시간 및 비용의 감소.

상위 레벨 VS. 하위 레벨

각 응답자가 다양한 PKI 지표와 관련하여 얼마나 잘 대응하는지/잘못 대응하는지 판단하기 위해 질문을 던졌습니다:

- 예상치 못한 인증서 만료로 인한 가동 중단을 방지함
- 필요 시 빠르게 인증서를 폐기함
- 디지털 인증서 관리의 효율성
- 부적절한 인증서 관리로 인한 보안 위험의 최소화
- 부적절한 인증서 관리로 인한 규제 준수 문제
- 비인가 인증서를 최소한으로 관리
- PKI 관련 SLA 충족
- PKI 발행 및 폐지 속도를 촉진함

잘한 대응/잘못한 대응을 바탕으로 각 질문에 대한 점수(긍정에서 부정까지)를 할당했습니다. 그런 다음 총점을 매겼습니다.

응답자의 대응 방법과 관련된 차이점을 파악하기 위하여 3개의 그룹으로 응답자들을 분류했습니다.

1 **리더**

이들 조직은 상기에 명시된 다양한 지표에서 최고 점수를 받았습니다.

2 **중간 그룹**

이들 조직은 상기에 명시된 다양한 지표에서 중간 점수를 받았습니다.

3 **하위 그룹**

이들 조직은 상기에 명시된 다양한 지표에서 최저 점수를 받았습니다.

그런 다음 리더와 하위 그룹을 비교하여 무슨 차이가 있는지, 그리고 리더의 차별점을 조사했습니다.

리더와 하위 그룹

응답자들은 그들이 직면하고 있는 PKI 관리 문제를 공개했습니다. 그들은 비인가 인증서, 예상치 못한 인증서 만료로 인한 운영 중단 등 기타 다양한 문제를 겪고 있습니다. 그러나 기업들이 겪는 문제의 수준은 같지 않았습니다. 따라서 응답자들을 3개의 그룹으로 나눠 상위 레벨과 하위 레벨을 비교했습니다. 그 차이점은 놀라웠습니다.

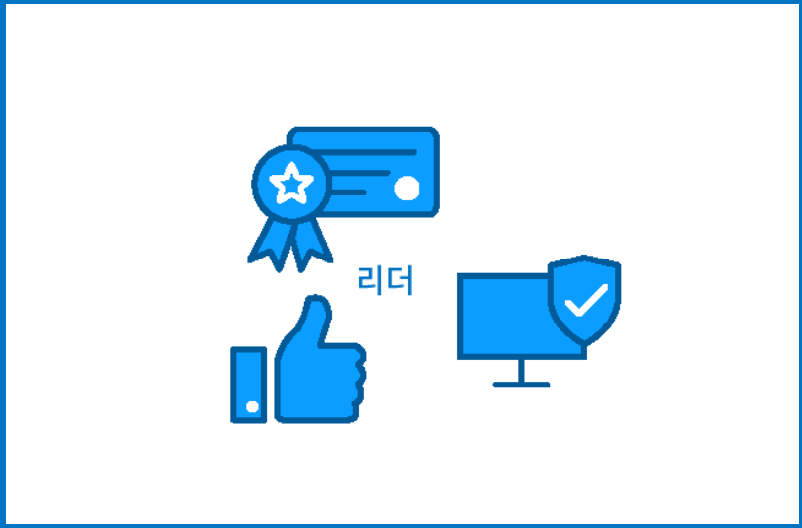
상위 레벨의 리더 그룹 적절히 대응하고 있었습니다. 특히, 상위 레벨의 1/3인 33%는 PKI 자동화를 우선 순위에 놓는 경향이 있다고 답했습니다. 리더 그룹은 다음 사항에 대해 2~3배 더 잘 대응합니다.

- PKI 보안 위험 최소화
- PKI 중단 시간 방지
- 비인가 인증서 최소화
- PKI SLA 준수
- 디지털 인증서 관리
- 인증서 발행 및 폐기
- 규정 준수

이와 반대로, 하위 그룹은 PKI 인증서 관리 기술의 부족으로 인해 심각한 불이익을 경험합니다. 그 불이익은 다음과 같습니다:

- 규정 준수 문제
- 보안 문제
- 생산성 손실
- 지연
- 과도한 워크로드
- 고객 이탈
- 수익 손실

리더 그룹이 앞서 나가는 이유는 무엇일까요? 이러한 PKI 리더로부터 어떤 교훈을 얻을 수 있을까요?



PKI 자동화 리더십 속성

PKI 리더는 PKI 인증서 관리에 소요된 시간에 대하여 2배 더 관심을 표명합니다. 이를 통해 PKI 관리에 집중할 수 있습니다. 두 번째, 비인가 인증서 문제를 더 많이 우려합니다. 세 번째로 리더 그룹은 PKI 자동화가 조직의 미래를 위해 중요하다고 생각합니다. 따라서 PKI 자동화를 이미 구현했을 가능성이 6배 정도 높습니다. 그렇다면 어떤 교훈을 배우고 어떻게 차별화할 수 있습니까?

거친 서부 시대

데이터를 깊게 들여다 보면 흥미로운 점을 발견할 수 있습니다. 서류 상 PKI 인증서 관리가 용이했던 것으로 보였던 그룹이 인증서 관리에 어려움을 겪는 경향을 보였습니다.

예를 들어, 더 적은 인증서를 관리하는 기업들은 예상치 못한 인증서 만료로 인한 운영 중단을 더 많이 경험할 가능성이 더 높았습니다. 또한, 다양한 PKI 관리 지표가 전체적으로 좋지 않습니다.

이는 '소량 PKI 인증서'를 보유한 기업이 대량 인증서 보유 기업에 비하여 매우 적은 개수의 인증서를 관리하고 있음에도 PKI 관리에 더 큰 관심을 가져야 함을 의미합니다. 예를 들어 소량 인증서 관리 기업 중 거의 50%가 PKI 인증서 관리 소요 시간에 대해 우려하고 있다고 답했습니다. 또한, 그들은 PKI 자동화 프로그램에 따른 인증서를 거의 2배 가까이 공유합니다.

처음에 이는 모순적인 상황으로 보였습니다. 그러나 소량 관리 기업의 PKI 관리 스킬이 부족한 것은 사실입니다. 흔히 100,000개 이상의 인증서를 관리하는 대량 관리 기업은 PKI 인증서 관리 방법에 있어 매우 노련한 반면 소량 관리 기업은 거친 서부와 같이 험난합니다. 정해진 규칙이 없으며 모든 사람이 자신의 방식으로 인증서를 관리합니다.

소량 관리 기업이 처한 상황은 거친 서부와 같이 험난합니다. 정해진 규칙이 없으며 모든 사람이 자신의 방식으로 인증서를 관리합니다.

PKI 자동화 리더십 속성

PKI 관리 리더 그룹은 인증서 재고에 더 관심을 기울이며, 역설적으로 관심을 적게 기울이는 그룹에 비하여 자신의 수준을 더 낮게 평가합니다. 그러나 이러한 그룹은 인증서 관련 운영 중단 또는 비인가 인증서 문제를 더 적게 보고하고 있으며, 이는 그들이 예상하는 것보다 더 잘 대응하고 있음을 시사합니다.

모순적인 자체 평가

다른 흥미로운 사실은 PKI 인증서 관리에 가장 관심을 기울이고 있는 기업들 사이의 차이점입니다. 상황을 객관적으로 평가하는 기업은 문제가 더 적었지만, 주관적으로 판단하는 기업은 대응 수준이 낮았습니다.

예를 들어, PKI 관리가 문제라고 생각할 가능성이 높은 기업을 가정해 보겠습니다. 이러한 기업은 새로운 인증서 발행의 속도, 인증서 구성의 실패, 비인가 인증서 발견, 기타 인증서 문제를 매우 우려하고 있다고 말할 가능성이 5배 더 높습니다.

그러나 실제로 비인가 인증서 문제를 보고하는 경우는 매우 낮습니다(관심이 없는 기업에 비하여 2/3 수준). 또한, 인증서 만기 사고와 관련된 운영 중단을 훨씬 적게 경험합니다(관심이 없는 기업의 3~5회 운영 중단과 비교하여 6개월 동안 1건의 운영 중단 사건).

또한, 보안 관련 설문조사에서도 이러한 현상이 나타납니다. 이 문제에 긴밀한 관심을 기울이는 기업들은 스스로의 단점과 실책을 대부분 인지하고 있기 때문에 큰 관심이 없는 기업에 비하여 자신을 더 가혹하게 평가하는 경향이 있습니다. 하지만 무관심 그룹에 비해 긴밀하게 관심을 기울이고 훨씬 잘 대응합니다.

PKI 인증서 관리의 객관성을 가장 우려하고 있는 기업은 문제 발생이 적었으나, 주관적으로 자체 평가한 기업들은 그렇지 못합니다.

권장 사항

PKI 인증서 카탈로그를 통하여 자동화를 적용하면 짧은 검증 기간, 진화된 암호화 표준, 조직 전반에 걸친 비즈니스 프로세서에서 디지털 인증서의 광범위한 채택을 포함한 많은 장점을 누릴 수 있습니다. 하지만 기업은 자동화 이니셔티브를 시작할 때 무엇을 고려해야 할까요? 자동화가 인증서 관리 목표를 지원하는 단계별 체크리스트는 다음과 같습니다.

인증서 관리

식별
인증서의 재고를 식별하고 생성합니다.

교정
기업 정책에 부합하지 않는 키와 인증서를 교정합니다.

보호
발행 및 폐지에 대한 최상의 관행을 보호합니다. 등록, 발행, 갱신을 표준화 및 자동화합니다.

모니터링
새로운 변경 사항을 모니터링합니다.

인증서 워크플로 자동화

식별
통제되지 않거나, 수동 관리되는 인증서 워크플로를 식별합니다.

채택
인증서 워크플로를 집중시키고 관리하는 소프트웨어를 포함하여 자동화를 채택합니다.

모니터링하기
중앙 집중식 가시성으로 모니터링하고 제어합니다.

공통 인증서 워크플로

- 웹 서버
- 장치 ID 및 관리
- 코드 서명
- 디지털 서명
- ID 및 액세스

조사 방법

텍사스주 댈러스에 위치한 ReRez Research는 북미, EMEA, 아시아 태평양, 라틴 아메리카 지역에서 1,000명 이상의 직원을 보유한 400여 곳의 기업 내 IT 전문가에 대한 설문조사를 수행했습니다. 응답자에는 IT 담당 이사, IT 보안 관리자, IT 기술자가 포함되었습니다. 주로 사용자, 서버, 모바일 장치에 대한 디지털 인증서를 관리하는 IT 전문가를 인터뷰했으며 중소기업과 대기업을 조사했습니다.

DigiCert PKI 자동화 전문가에게 연락하여 조직의 니즈를 평가하고 맞춤형 솔루션에 대해 상담하십시오. 여기에서 PKI 배포를 자동화하는 방법에 대해 자세히 알아보세요.