네트워크 보안 정책:모범 사례 백서

목차

소개

보안 정책이 없으면 네트워크의 가용성이 손상될 수 있습니다.이 정책은 네트워크에 대한 위험을 평가하고 응답할 팀을 구축하는 것으로 시작합니다.정책을 계속 사용하려면 보안 변경 관리 방식을 구현하고 보안 위반에 대해 네트워크를 모니터링해야 합니다.마지막으로, 검토 프로세스는 기존 정책을 수정하고 학습한 교훈을 적용합니다.

이 문서는 다음 세 가지 영역으로 구성됩니다.준비, 예방 및 대응.이러한 각 단계를 자세히 살펴보겠습니다.

준비

보안 정책을 구현하기 전에 다음을 수행해야 합니다.

- 사용 정책 문을 만듭니다.
- 위험 분석을 수행합니다.
- 보안 팀 구조를 설정합니다.

사용 정책 명령문 생성

보안과 관련된 사용자의 역할과 책임을 개괄적으로 설명하는 사용 정책 문을 작성하는 것이 좋습니다.먼저 회사 내의 모든 네트워크 시스템과 데이터를 포괄하는 일반적인 정책으로 시작할 수 있습니다.이 문서에서는 일반 사용자 커뮤니티에서 보안 정책, 목적, 보안 업무 개선 지침 및 보안 책임 정의에 대한 이해를 제공해야 합니다.귀사가 직원에게 징벌적 또는 징계 조치를 가할 수 있는 특정 조치를 파악한 경우, 이러한 조치 및 이를 피하는 방법을 이 문서에 명시해야 합니다.

다음 단계는 파트너가 이용할 수 있는 정보, 해당 정보의 예상 처분, 회사의 직원 행동에 대한 이해를 파트너에게 제공할 수 있는 파트너 이용 가능 사용 명세서를 작성하는 것입니다.보안 공격으로 식별된 특정 행위 및 보안 공격이 탐지될 경우 취해질 징벌적 조치를 명확하게 설명해야 합니다.

마지막으로, 사용자 계정 관리, 정책 시행 및 권한 검토에 대한 절차를 설명하는 관리자 수락 가능한 사용 명령문을 생성합니다.회사에서 사용자 암호 또는 후속 데이터 처리와 관련된 특정 정책을 가지고 있는 경우, 이러한 정책도 명확하게 제시합니다.파트너 수락 가능 한 사용 및 사용자 수락 가능 한 사용 정책 정책에 대한 정책을 확인 하여 균일성을 보장 합니다.허용 가능한 사용 정책에 나열된 관리자 요구 사항이 교육 계획 및 성과 평가에 반영되었는지 확인합니다.

위험 분석 수행

위험 분석은 네트워크, 네트워크 리소스 및 데이터에 대한 위험을 식별합니다.이는 네트워크에 대한 모든 가능한 진입점 또는 가능한 모든 공격 수단을 식별해야 한다는 의미는 아닙니다.위험 분석의 목적은 네트워크의 일부를 식별하고, 각 부분에 위협 등급을 할당하고, 적절한 수준의 보안을 적용하는 것입니다.이를 통해 보안과 필수 네트워크 액세스 간의 적절한 균형을 유지할 수 있습니다.

각 네트워크 리소스를 다음 3가지 위험 레벨 중 하나를 할당합니다.

- **위험도가 낮은** 시스템 또는 데이터(권한이 없는 사람이 열람한 데이터, 데이터 손상 또는 데이터 손실)는 비즈니스에 지장을 주거나 법적 또는 재정적 영향을 주지 않습니다.대상 시스템이나 데이터를 쉽게 복원할 수 있으며 다른 시스템에 대한 추가 액세스를 허용하지 않습니다.
- **중간 위험** 시스템 또는 데이터(권한이 없는 사람이 보는 데이터, 데이터 손상 또는 데이터가 손실됨)는 업무 중단, 경미한 법적 또는 재정적 파급, 기타 시스템에 대한 추가 액세스를 제공할 수 있습니다.대상 시스템이나 데이터를 복구하기 위해서는 보통 정도의 노력이 필요하며 복원 프로세스는 시스템을 중단시킵니다.
- **고위험** 시스템 또는 데이터(권한이 없는 사용자가 조회한 데이터, 데이터 손상 또는 데이터 손실)는 비즈니스에 심각한 지장을 주거나, 중대한 법적 또는 재정적 영향을 주거나, 사람의 건강과 안전을 위협하는 데이터.대상 시스템이나 데이터를 복구하기 위해서는 상당한 노력이 필요하며, 그렇지 않으면 복원 프로세스가 비즈니스나 기타 시스템에 지장을 초래합니다.

다음 각 항목에 위험 레벨을 할당합니다.코어 네트워크 장치, 배포 네트워크 장치, 액세스 네트워크 장치, 네트워크 모니터링 장치(SNMP 모니터 및 RMON 프로브), 네트워크 보안 장치(RADIUS 및 TACACS), 이메일 시스템, 네트워크 파일 서버, 네트워크 인쇄 서버, 네트워크 응용 프로그램 서버(DNS 및 DHCP), 데이터 응용 프로그램 서버(Oracle 또는 기타 독립형 응용 프로그램), 데스크톱 컴퓨터 및 기타 장치(독립형 인쇄 서버 및 네트워크 컴퓨터)

스위치, 라우터, DNS 서버 및 DHCP 서버와 같은 네트워크 장비는 네트워크에 대한 추가 액세스를 허용할 수 있으므로 중급 또는 고위험 디바이스입니다.이 장비가 손상되면 네트워크 자체가 붕괴될 수도 있습니다.이러한 실패는 비즈니스에 큰 지장을 초래할 수 있습니다.

위험 수준을 할당한 후에는 해당 시스템의 사용자 유형을 확인해야 합니다.가장 일반적인 사용자 유형은 다음과 같습니다.

- **관리자** 네트워크 리소스를 담당하는 내부 사용자
- **액세스**가 더 큰 권한이 필요한 권한이 있는 내부 사용자
- **사용자** 일반 액세스 권한이 있는 내부 사용자
- **파트너** 일부 리소스에 액세스해야 하는 외부 사용자
- **기타** 외부 사용자 또는 고객

각 네트워크 시스템에 필요한 위험 수준 및 액세스 유형을 식별하면 다음 보안 매트릭스의 기반이 됩니다.보안 매트릭스는 각 시스템에 대한 빠른 참조 및 네트워크 리소스에 대한 액세스를 제한하

기 위한 적절한 전략을 생성하는 등 추가 보안 조치를 위한 시작점을 제공합니다.

시스템	설명	위험 수준	사용자 유형
ATM 스위치	코어 네트워크 장치	높음	디바이스 컨피그레이션 관리자(지원 직원만 해당),다른 모든 항목은 전송으로 사용
네트워크 라우터	배포 네트워크 장치	높음	디바이스 컨피그레이션 관리자(지원 직원만 해당),다른 모든 항목은 전송으로 사용
클로짓 스위치	네트워크 장치 액세스	중간	디바이스 컨피그레이션 관리자(지원 직원만 해당),다른 모든 항목은 전송으로 사용
ISDN 또는 전화 접속 서버	네트워크 장치 액세스	중간	디바이스 컨피그레이션 관리자(지원 직원만 해당),특별 액세스를 위한 파트너 및 권한 있는 사용자
방화벽	네트워크 장치 액세스	높음	디바이스 컨피그레이션 관리자(지원 직원만 해당),다른 모든 항목은 전송으로 사용
DNS 및 DHCP 서버	네트워크 애플리케이션	중간	구성 관리자일반 사용자 및 사용 권한 있는 사용자
외부 전자 메일 서버	네트워크 애플리케이션	낮음	구성 관리자인터넷과 내부 메일 서버 간의 메일 전송을 위한 기타 모든 기능
내부 이메일 서버	네트워크 애플리케이션	중간	구성 관리자사용할 기타 모든 내부 사용자
Oracle 데이터베이스	네트워크 애플리케이션	보통 또는 높음	시스템 관리 관리자데이터 업데이트에 대한 권한이 있는 사용자데이터 액세스를 위한 일반 사용자부분 데이터 액세스를 위한 기타 모든 기능

보안 팀 구조 설정

Security Manager가 이끄는 부서간 보안 팀을 각 회사의 운영 영역 참석자와 함께 만듭니다.팀 담당자는 보안 정책 및 보안 설계 및 구현의 기술적 측면을 알아야 합니다.팀 구성원에게 추가 교육이 필요한 경우가 많습니다.보안 팀에는 세 가지 책임 영역이 있습니다.정책 개발, 실행 및 대응

정책 개발에서는 회사의 보안 정책 수립 및 검토에 중점을 둡니다.최소한 매년 위험 분석 및 보안 정책을 검토합니다.

보안 팀이 위험 분석을 수행하고, 보안 변경 요청을 승인하며, 벤더와 CERT 메일 목록에서 보안 알림을 검토하며, 일반 언어 보안 정책 요구 사항을 특정 기술 구현으로 전환하는 단계입니다.

마지막 책임은 응답이다.네트워크 모니터링에서는 보안 위반을 식별하는 경우가 많으나, 이러한 위반을 실제로 트러블슈팅하고 수정하는 보안 팀 멤버입니다.각 보안 팀 구성원은 자신의 운영 영역에서 장비가 제공하는 보안 기능을 자세히 알아야 합니다.

팀의 책임을 전체적으로 정의했지만 보안 정책에서 보안 팀 구성원의 개별 역할과 책임을 정의해야 합니다.

방지

방지는 두 부분으로 나눌 수 있습니다.보안 변경 승인 및 네트워크 보안 모니터링.

보안 변경 승인

보안 변경은 네트워크의 전반적인 보안에 영향을 미칠 수 있는 네트워크 장비 변경으로 정의됩니다.보안 정책은 기술 이외의 용어로 특정 보안 구성 요구 사항을 식별해야 합니다.즉, "외부 소스 FTP 연결이 방화벽을 통해 허용될 수 없음"이라는 요구 사항을 정의하는 대신 "외부 연결이 내부 네트워크에서 파일을 검색할 수 없어야 함"으로 요구 사항을 정의합니다. 조직의 고유한 요구 사항 집합을 정의해야 합니다.

보안 팀은 일반 언어 요구 사항 목록을 검토하여 요구 사항을 충족하는 특정 네트워크 구성 또는 설계 문제를 식별해야 합니다.팀에서 보안 정책을 구현하기 위해 필요한 네트워크 컨피그레이션 변경 사항을 만들었으면 향후 컨피그레이션 변경 사항에 적용할 수 있습니다.보안 팀에서 모든 변경 사항을 검토할 수 있지만, 이 프로세스를 통해 특별한 치료를 받을 수 있는 위험을 충분히 제기하는 변경 사항만 검토할 수 있습니다.

보안 팀은 다음 유형의 변경 사항을 검토하는 것이 좋습니다.

- 방화벽 컨피그레이션을 변경합니다.
- ACL(Access Control List)에 대한 변경 사항
- SNMP(Simple Network Management Protocol) 컨피그레이션의 변경 사항
- 승인된 소프트웨어 수정 레벨 목록과 다른 소프트웨어의 변경 또는 업데이트

또한 다음 지침을 준수하는 것이 좋습니다.

- 정기적으로 네트워크 디바이스에 대한 비밀번호를 변경합니다.
- 네트워크 디바이스에 대한 액세스를 승인된 인력 목록으로 제한합니다.
- 네트워크 장비 및 서버 환경의 현재 소프트웨어 수정 수준이 보안 구성 요구 사항을 준수하는지 확인합니다.

이러한 승인 지침 외에도, 보안 팀의 담당자가 변경 관리 승인 보드에 앉아 이사회의 모든 변경 사항을 모니터링하도록 합니다.보안 팀 담당자는 보안 팀에서 승인하기 전까지 보안 변경으로 간주되는 변경 사항을 거부할 수 있습니다.

네트워크 보안 모니터링

보안 모니터링은 네트워크 모니터링과 유사하지만, 보안 위반을 나타내는 네트워크의 변경 사항을 탐지하는 데 초점을 둡니다.보안 모니터링의 시작점은 위반 사항을 결정하는 것입니다.위험 분석 수행에서 시스템에 대한 위협을 기준으로 필요한 모니터링 수준을 파악했습니다.보안 변경 승인에서 네트워크에 대한 특정 위협을 식별했습니다.이 두 가지 매개 변수를 모두 살펴봄으로써 모니터

링해야 할 사항과 모니터링 빈도를 명확하게 파악할 수 있습니다.

Risk Analysis Matrix에서 방화벽은 위험이 높은 네트워크 디바이스로 간주되며, 이는 방화벽을 실시간으로 모니터링해야 함을 나타냅니다.Approving Security Changes(보안 변경 승인) 섹션에서 방화벽의 변경 사항을 모니터링해야 한다는 것을 확인할 수 있습니다.즉, SNMP 폴링 에이전트는 실패한 로그인 시도, 비정상적인 트래픽, 방화벽 변경, 방화벽에 부여된 액세스, 방화벽을 통해 설정된 연결 등과 같은 사항을 모니터링해야 합니다.

다음 예에서는 위험 분석에서 식별된 각 영역에 대한 모니터링 정책을 생성합니다.저희는 위험이 낮은 장비를 매주, 중급 장비를 매일, 그리고 위험이 높은 장비를 매시간 모니터링하는 것이 좋습니다.더 신속한 탐지가 필요한 경우 더 짧은 시간대를 모니터링하십시오.

마지막으로 보안 정책은 보안 팀에 보안 위반을 알리는 방법을 해결해야 합니다.네트워크 모니터링 소프트웨어가 위반을 가장 먼저 탐지하는 경우가 많습니다.운영 센터에 알림을 트리거해야 하며, 필요한 경우 호출기를 사용하여 보안 팀에 알려야 합니다.

응답

응답은 다음 세 부분으로 나눌 수 있습니다.보안 위반, 복원 및 검토.

보안 위반

위반이 탐지되면 네트워크 장비를 보호하고, 침입 범위를 결정하고, 정상적인 운영을 복구할 수 있는 능력은 빠른 결정에 따라 달라집니다.이러한 결정을 미리 내리면 침입에 훨씬 더 쉽게 대응할 수 있습니다.

침입 탐지 후 첫 번째 작업은 보안 팀의 알림입니다.절차도 없이, 올바른 사람들이 올바른 반응을 적용하도록 하는 것은 상당한 지연이 있을 것이다.보안 정책에서 하루 24시간, 일주일 7일 사용 가능한 절차를 정의합니다.

그런 다음 보안 팀에 주어진 권한 수준을 정의하여 변경을 수행하고 변경할 순서를 지정해야 합니다.가능한 수정 조치는 다음과 같습니다.

- 위반에 대한 추가 액세스를 방지하기 위한 변경 사항 구현
- 위반된 시스템을 격리합니다.
- 공격을 추적하기 위해 통신업체 또는 ISP에 문의합니다.
- 기록 장치를 사용하여 증거 수집
- 위반된 시스템 또는 위반 소스의 연결을 끊습니다.
- 경찰이나 다른 정부 기관 문의
- 위반된 시스템을 종료하는 중입니다.
- 우선 순위 목록에 따라 시스템을 복원합니다.
- 내부 관리 및 법무 담당자에게 통보

보안 정책에서 관리 승인 없이 수행할 수 있는 모든 변경 사항을 자세히 설명해야 합니다.

마지막으로, 보안 공격 중에 정보를 수집하고 유지 관리해야 하는 2가지 이유가 있습니다.보안 공격에 의해 시스템이 감염되는 정도를 확인하고 외부 위반을 기소합니다.정보의 유형 및 수집 방식은 목표에 따라 달라집니다.

위반 범위를 확인하려면 다음을 수행합니다.

- 네트워크의 스니퍼 추적, 로그 파일의 복사본, 활성 사용자 계정 및 네트워크 연결을 얻어 이벤트를 기록합니다.
- 계정을 비활성화하고, 네트워크 장비를 네트워크에서 분리하고, 인터넷에서 연결을 끊음으로써 추가 보안 침해를 제한합니다.
- 손상 및 공격 방법에 대한 자세한 분석을 위해 손상된 시스템을 백업합니다.
- 다른 보안 침해 징후를 찾아보십시오.시스템이 손상된 경우 다른 시스템이나 어카운트가 관련된 경우가 많습니다.
- 보안 디바이스 로그 파일 및 네트워크 모니터링 로그 파일이 공격 방법에 대한 단서를 제공하는 경우가 많으므로 이를 유지 관리하고 검토합니다.

법적 조치를 취하고자 하는 경우, 법무팀에 증거수집 및 당국의 개입에 대한 절차를 검토하도록 하십시오.이러한 검토는 법적 절차에서의 증거의 효과를 증가시킨다.위반이 본질적으로 내부적인 것이면 인사부에 문의하십시오.

복원

정상적인 네트워크 운영 복원은 보안 위반 대응에 대한 최종 목표입니다.보안 정책에서 일반적인 백업을 수행, 보호 및 제공하는 방법을 정의합니다.각 시스템에는 고유한 백업 수단 및 절차가 있으므로 보안 정책은 각 시스템에 대해 백업에서 복원해야 하는 보안 조건을 자세히 설명하는 메타 정책 역할을 해야 합니다.복원 작업을 수행하기 전에 승인이 필요한 경우 승인 절차를 포함합니다.

검토

검토 프로세스는 보안 정책을 생성하고 유지 관리하는 최종 작업입니다.다음 세 가지 사항을 검토해야 합니다.정책, 상태 및 업무 수행

보안 정책은 끊임없이 변화하는 환경에 적응하는 살아있는 문서여야 합니다.알려진 모범 사례에 대한 기존 정책을 검토하여 네트워크를 최신 상태로 유지합니다.또한 CERT 웹 사이트 에서 보안 정책에 통합할 수 있는 유용한 팁, 사례, 보안 개선 및 알림을 확인하십시오.

또한 원하는 보안 상태와 비교하여 네트워크의 상태를 검토해야 합니다.보안 전문 외부 기업은 네트워크에 침투하여 네트워크 상태뿐만 아니라 조직의 보안 대응도 테스트할 수 있습니다.고가용성 네트워크의 경우 매년 이러한 테스트를 수행하는 것이 좋습니다.

마지막으로, 연습은 보안 위반 시 수행할 작업을 명확하게 파악할 수 있도록 지원 인력의 드릴이나 테스트로 정의됩니다.이 드릴은 종종 관리 부서에서 예고하고 네트워크 상태 테스트와 함께 수행됩니다.이 검토에서는 수정 조치를 취할 수 있도록 인력 교육 및 절차의 허점을 파악합니다.

관련 정보

- 기타 모범 사례 백서
- Technical Support - Cisco Systems