KRITIS UND DAS NEUE IT-SICHERHEITSGESETZ

Sicherheit beginnt bei der Infrastruktur

TEST DRIVE!

NUTANIX
YOUR ENTERPRISE CLOUD

SICHERHEIT BEGINNT BEI DER INFRASTRUKTUR

Die zurückliegenden Monate haben uns gezeigt, wie wichtig die sogenannten kritischen Infrastrukturen sind. Staat, Verwaltung und das Gesundheitswesen müssen unbedingt funktionieren, in normalen wie in Krisenzeiten. Damit dies der Fall ist, verlangt der Gesetzgeber zurecht, kritische Infrastrukturen effektiv und effizient vor Hackerangriffen oder Attacken mit Erpressersoftware zu schützen. IT-Sicherheit ist jedoch nicht nur eine Frage der richtigen IT-Sicherheitssoftware, sondern muss als holistischer Ansatz begriffen werden. Effektive Sicherheit beginnt daher schon bei der Infrastruktur.

Es ist kein Zufall, dass das aktuelle IT-Sicherheitsgesetz mehr Pflichten als seine Vorgänger kennt und mehr Unternehmen und Bereiche seinen Vorgaben unterwirft als bisher. So gehören jetzt zum Beispiel auch Entsorger oder Unternehmen mit hoher volkswirtschaftlicher Bedeutung, darunter Hersteller von IT-Produkten zur Verarbeitung von Verschlusssachen, zum Kreis der kritischen Infrastrukturen. Schließlich waren die Angriffe staatlicher wie privater Akteure noch nie so zahlreich und abgefeimt wie heute. Nicht auszudenken, was passieren würde, wenn Cyberkriminelle die Kontrolle über Atomanlagen oder die Energie- und Wasserversorgung Deutschlands übernehmen würden.

Wir müssen ehrlich sein: 100 Prozent IT-Sicherheit gibt es nicht. Fehler sind der Software inhärent. Und je mehr wir von den Vorteilen der Digitalisierung profitieren wollen, desto mehr Software werden wir nutzen und entwickeln. Dabei werden immer wieder Sicherheitslücken entstehen. Und da reparieren immer schwieriger und aufwändiger ist als vorbeugen, kommt es vor allem auf drei Dinge an: Zum einen muss schon bei der Entwicklung von Softwarecode die Zahl der möglichen Sicherheitslücken durch geeignete Maßnahmen und Prozesse minimiert werden. Zum anderen müssen sich Applikationen und Systemsoftware viel einfacher und häufiger als bisher aktualisieren und patchen lassen. Drittens müssen sich die betroffenen Systeme, Applikationen und Daten im Fall der Fälle verlustfrei und in der kürzest möglichen Zeit wiederherstellen lassen.

DREI-SCHICHTEN-ARCHITEKTUR: HINDERNIS FÜR SCHNELLES PATCHEN

Das Aktualisieren und Patchen erfordert in einer herkömmlichen Drei-Schichten-Architektur wegen der Vielzahl an involvierten Herstellern und der Unterschiedlichkeit ihrer Technologien sehr viel Zeit und verursacht hohe Kosten. Eine IT-Infrastruktur aus einem Guss hingegen, komplett virtualisiert und ausschließlich softwaregestützt und -gesteuert, kann diese Kosten deutlich reduzieren – ohne dass Abstriche bei der Sicherheit und Hochverfügbarkeit zu befürchten wären. Voraussetzung dafür ist jedoch, dass im Design einer solchen Infrastruktur die Sicherheit gleichsam eingebaut ist, in allen Phasen der Entwicklung und Weiterentwicklung.

Idealerweise ist Security in einer solchen softwaregestützten Infrastruktur eine neben anderen gleichberechtigte Funktionalität, die den gesamten Prozess einer auf Sicherheit ausgelegten Entwicklung abbildet. Dieser Prozess reicht vom Entwurf und Einsatz der Software bis hin zum Test und ihrem zusätzlichen „Härten". Im Rahmen eines solchen „Security Development Lifecycle" (SecDL) wird der Programmcode systematisch nach Sicherheitslücken untersucht. Werden die Entwickler fündig, machen sie sich unverzüglich daran, sie zu beseitigen. Diese iterative Vorgehensweise zieht sich durch den kompletten Lebenszyklus in der Softwareentwicklung und besteht aus den Schritten: Bewerten, messen, berichterstatten, testen, aktualisieren und dann das Ganze wieder von vorn.

In diesem Prozess sind aber nicht nur Sicherheitslücken aufzuspüren, sondern auch verschiedene Regelwerke zu berücksichtigen, um Sicherheitsauflagen zu erfüllen. Dazu zählt zum Beispiel die vom BSI anerkannte Zertifizierung nach dem Standard ISO/IEC 15408 (Common Criteria) in der Version 3.1 für das Bewertungssicherheitsniveau EAL2+. Als weitere Regularien wären etwa FIPS 140-2, NIST-SP800-131A, NSA Suite B Support, Section 508 VPAT und TAA Compliant zu nennen.

SICHERHEIT: EINE FRAGE DER ARCHITEKTUR

Diese Anforderungen lassen sich jedoch mit klassischen Drei-Schichten-Architekturen von Rechenzentrumsinfrastrukturen nur mit einem immensen technischen, personellen und finanziellen Aufwand erfüllen. Damit stellt das Thema IT-Sicherheit unmittelbar die Frage nach der richtigen IT-Architektur, die ein höheres Schutzniveau ermöglicht und bewirkt. Denn klassische Infrastrukturen mit ihren Komponenten Netzwerke, Speicher, Rechenleistung und Virtualisierung bieten kriminellen Hackern und Spionen zahlreiche und nur schwer zu schließende Einfallstore dar.

Zum Glück haben Rechenzentrumsinfrastrukturen in den vergangenen Jahren mittels Softwaresteuerung massive Fortschritte gemacht. Dabei wurde die Idee der Servervirtualisierung erfolgreich auf die anderen Komponenten der Infrastruktur übertragen und angewandt. Fachleute sprechen in diesem Zusammenhang von Hyperkonvergenz, die sämtliche Infrastrukturelemente zu integrierten Funktionalitäten ein und derselben Softwareschicht transformiert und sie damit vollständig von der darunterliegenden Hardwareschicht löst. Das ist der Stand der Technik, den das IT-Sicherheitsgesetz und die darauf verweisende BSI-Verordnung voraussetzen und einfordern. Und das ist der Stand der hyperkonvergenten Infrastruktursoftware (HCI) von Nutanix.

SOFTWARE: MEHR SICHERHEIT DANK AUTOMATISIERUNG

In der Regel zwingen zeitliche Restriktionen und der Primat eines möglichst effizienten IT-Betriebs die IT-Verantwortlichen dazu, auf häufige und zeitnahe Sicherheitsaktualisierungen zu verzichten. Doch auch diese Herausforderung kann eine hyperkonvergente Infrastruktursoftware meistern, zumindest die HCI-Software von Nutanix.

Denn mit HCI von Nutanix lassen sich auf Basis von XCCDF (Extensible Configuration Checklist Description Format) Sicherheits-Checklisten, Benchmarks und ähnliche Dokumente erstellen. XCCDF ist maschinenlesbar und eignet sich daher sehr gut für die Implementierung von Sicherheitsleitfäden, sogenannten Security Technical Implementation Guides (STIGs). Mit Nutanix lassen sich die darin beschriebenen Aufgaben automatisch ausführen. Diese Automatisierung bietet die folgenden Vorteile:

- Der „maschinenlesbare“ STIG kann von automatisierten Assessment-Tools genutzt werden und führt damit zu einer schnelleren Validierung und Akkreditierung. Die Praxis zeigt, dass sich der dafür notwendige Zeitaufwand von 9 bis 12 Monaten je nach Fall bis auf wenige Minuten reduzieren lässt.

- Produktivsysteme lassen sich über Selbstheilungsfunktionen wieder in einen ordnungsgemäßen Zustand überführen und stellen dabei das Einhalten der Compliance-Vorgaben sicher.

- Sich selbst verschlüsselnde Laufwerke ermöglichen eine „Data at Rest Encryption”-Funktionalität. Damit lässt sich ein Datenschutzniveau nach den Vorgaben „FIPS 140-2 Level 2 Compliance“ erzielen.

- Bei einer starken Verschlüsselung dürfen sich die Schlüssel nicht auf der zu schützenden Infrastruktur befinden. Vielmehr braucht es ein Zusammenspiel mit Key-Management-Servern von Drittherstellern. Die sich selbst verschlüsselnden Laufwerke von Nutanix erzeugen neue Schlüssel, die anschließend auf separate Key-Management-Server unter Verwendung des KMIP-Protokolls hochgeladen werden.

ZERO-TRUST SECURITY

Immer mehr KRITIS-Betreiber verfolgen einen Zero-Trust-Sicherheitsansatz. Nutanix ermöglicht heute schon Anomalieerkennung auf Basis von maschinellem Lernen und Diensten zur Bewertung von IP-Adressen. Dadurch lassen sich bekannte Angriffsvektoren, einschließlich potenzieller Erpressersoftware, auf Netzwerkebene entdecken, bevor sie die Anwendungs- und Datenschicht erreichen. Nutanix überwacht zudem Endpunkte, um Netzwerkverkehr aufzuspüren, der aus zweifelhaften Quellen stammt. Dies ist insbesondere für den Schutz virtueller Desktop-Infrastrukturen (VDI) geeignet, die ein primäres Ziel für die Erstinfektion und die Ausbreitung von Erpressersoftware darstellen.

Außerdem enthält die Nutanix-Software native Funktionen zur Erkennung von Ransomware. Spezielle Dateianalysefunktionen können abnormale und verdächtige Zugriffsmuster erkennen und bekannte Ransomware-Signaturen identifizieren. Dadurch lässt sich der Datenzugriff in Echtzeit blockieren. Zudem erstellt die Software unveränderbare Snapshots, also unveränderbare Kopien des Datenbestands. Das verhindert das Verfälschen und Löschen von Dateien durch Erpressersoftware oder Ransomware, deren Angriffe so konzipiert sind, dass sie auch die Dateisicherungen verschlüsseln und so die Wiederherstellung der Dateien verhindern. Für Dateilaufwerke hingegen, für die sie aktiviert wurden, sorgen die nativen Snapshot-Funktionen von Nutanix für eine beschleunigte Wiederherstellung, da die so gesicherten Dateien den Verschlüsselungsversuchen der Cyberkriminellen entzogen sind. Mit Hilfe dieser vollständig integrierten Funktionalitäten können IT-Profis Angriffe mit Erpressersoftware sowohl entdecken als auch schnell die Folgen davon beseitigen.

NULLTOLERANZ DURCH AUTOMATISIERTES REGELWERK

Bei einem Zero-Trust-Sicherheitsansatz jedoch kann die Entwicklung eines entsprechenden Regelwerks, das sowohl effizient als auch effektiv ist, eine erhebliche Hürde darstellen. Nutanix wird demnächst Funktionalitäten bieten, mit deren Hilfe sich diese weit verbreitete Herausforderung meistern und automatisch Regeln für die Mikrosegmentierung in KRITIS-Netzwerken erstellen lassen. Dies wird eine Planungs-Engine ermöglichen, die mittels maschinellen Lernens den Netzwerkverkehr analysiert und Sicherheitsregeln vorschlägt, um VM-Workloads vor potentiellen Angriffen zu schützen.

Darüber hinaus ist die Integration der Nutanix-Software mit der branchenführenden Lösung für Vulnerability Management Detection and Response (VMDR) von Qualys Inc. geplant. Durch die Bedrohungserkennung auf der Ebene der virtuellen Maschinen und die Visualisierung des Risikos von Sicherheitslücken sollen Kunden in die Lage versetzt werden, ihre Patch-Prozesse zum Schließen von Sicherheitslücken zu optimieren. Verbesserte Schutzmechanismen in der Nutanix-Funktionalität für Dateimanagement werden dabei helfen, Angriffsversuche mit Hilfe von mehr als 4.000 bekannten Signaturen von Erpressersoftware, die sich dynamisch aktualisieren lassen, zu entdecken und abzuwehren. Außerdem haben das Betriebssystem, der Hypervisor und die Dateimanagementfunktionalitäten von Nutanix erfolgreich die strengen Testverfahren des US-Verteidigungsministeriums zu Cybersicherheit und Interoperabilität durchlaufen und dürfen jetzt offiziell in der „Department of Defense Information Network Approved Products List (APL)“ geführt werden.

BUSINESS CONTINUITY UND DISASTER RECOVERY FÜR KRITISCHE INFRASTRUKTUREN

Nutanix-Kunden profitieren heute schon von Funktionalitäten für unterbrechungsfreien Geschäftsbetrieb und Disaster Recovery (DR), die bislang nur in Speziallösungen zur Verfügung standen. Dazu zählen auf Wunsch die Nutzung der Public Cloud als Sicherungsort, natives Metro-Clustering für den integrierten Nutanix-eigenen Hypervisor, was im Katastrophenfall ein automatisches Failover ermöglicht, und die durchgängige Verschlüsselung des DR-Datenverkehrs. Darüber hinaus verschafft ein neues DR-Dashboard eine umfassende Sicht auf DR-Konfiguration und -Status der Primär- und Sekundärstandorte der Kunden. Diese können dadurch auf spezielle DR-Hardware und -Software verzichten, Lizenzkosten senken, Wiederherstellungszeiten verkürzen, Betriebsabläufe vereinfachen und möglicherweise teure Sekundärstandorte im Hot-Standby-Modus einsparen. Zudem erhalten speziell mittelständische KRITIS-Unternehmen, die nicht über die notwendigen Mittel und Kenntnisse verfügen, um zuverlässige DR-Funktionalitäten zu implementieren, die Möglichkeit, ihr Geschäft besser vor Ausfällen und Unterbrechungen zu schützen.

SOFTWARESTEUERUNG: WEITERE VORTEILE

Weiterer Vorteil der vollständig softwaregestützten und -gesteuerten Infrastruktursoftware von Nutanix ist der Verzicht auf Spezialhardware, so dass sich KRITIS-Rechenzentren durchgängig mit handelsüblicher und damit deutlich günstigerer x86-Hardware ausrüsten lassen.

Möglich wird dies dank der Softwaresteuerung von Nutanix. Denn sie sorgt dafür, dass die Daten stets in der Nähe von Fachverfahren und sonstigen Anwendungen – von sicheren Telearbeitsplätzen bis zu Geoinformationssystemen und lastintensiven Datenbankumgebungen – sowie redundant vorgehalten werden. Das senkt den Platzbedarf, Netzwerkverkehr und Stromverbrauch im Rechenzentrum massiv. Spiegelbildlich dazu steigt die Ausfallsicherheit. Fallen Hardwarekomponenten aus, werden die Anwendungen, Dienste und Daten einfach auf andere Ressourcen verschoben, und das alles automatisch.

Steigt der Ressourcenbedarf, skaliert die hyperkonvergente Infrastruktursoftware von Nutanix linear. Zusätzliche Server, Hypervisoren, Speicher- und Rechenkapazitäten lassen sich im laufenden Betrieb hinzufügen und die Steuerungssoftware von Nutanix sorgt dafür, dass sie nahtlos in den allgemeinen Ressourcenpool integriert werden und damit für sämtliche Arbeitslasten zur Verfügung stehen.

OFFENHEIT STATT GRENZEN

Das Ziel von Software statt Hardware für mehr Sicherheit in kritischen Infrastrukturen wäre verfehlt, wenn sie den Entscheidern und Rechenzentrumsbetreibern jeglichen Handlungsspielraum nehme und Starrheit anstatt Flexibilität brächte. Nutanix verfolgt den Ansatz einer offenen Architektur. Sämtliche Komponenten sind über die Managementoberfläche mittels Programmierschnittstellen (APIs) ansprechbar. Schon heute bietet Nutanix Kooperationen mit Anbietern von Key-Management-Servern sowie von IT-Lösungen für Endpunktsicherheit inklusive der Absicherung mobiler Endgeräte.

Darüber hinaus unterstützt Nutanix verschiedenste Hardwareplattformen namhafter Hersteller wie Dell, HPE oder Fujitsu und viele andere. Zudem haben Kunden die Wahl zwischen den gängigen Hypervisoren von VMware und Microsoft oder AHV von Nutanix. Mehr Wahlfreiheit geht nicht!

DATENHOHEIT UND -SICHERHEIT

Mit der Softwaresteuerung von Nutanix behalten KRITIS-Betreiber stets die volle Datenhoheit. Sie allein bestimmen, wo ihre Daten gespeichert, verarbeitet und verwaltet werden. Darüber hinaus sorgt der Anbieter von Anfang an für größtmögliche Datensicherheit. Das gilt bereits für die Entwicklung und setzt sich bis zu Sicherheitsmechanismen auf Netzwerkebene fort. Diese helfen unter anderem zu verhindern, dass sich Angreifer seitwärts im Netz bewegen. Auch bei Verlagerungen von Anwendungen und Servern nehmen diese ihren Schutz gleichsam mit sich mit.

BETRIEBS- STATT KAPITALKOSTEN

Nutanix sorgt nicht nur für die Portierbarkeit von Anwendungen und Diensten, sondern auch der Abrechnungsmodelle. Diese enthalten neben Lizenzen auch Abonnements, so dass Anfangsinvestitionen entfallen. Der finanzielle Aufwand verlagert sich damit von den Kapital- (CAPEX) zu den Betriebskosten (OPEX).

EIN STARKER PARTNER FÜR KRITIS-BETREIBER

Als börsennotiertes Unternehmen mit mehr als 20.000 Kunden weltweit, über 6.000 Mitarbeiterinnen und Mitarbeitern – davon allein 16 Prozent im Support – und einem Umsatz von rund 1,4 Mrd. US-Dollar im Geschäftsjahr 2021 steht Nutanix für Investitionssicherheit. Kein Wunder, dass Ministerien und Behörden von der kommunalen bis zur Bundesebene, Organisationen und Unternehmen des öffentlichen Sektors inklusive Gesundheitswesen und Versorger Nutanix-Lösungen in großem Maßstab nutzen – und das zu vollster Zufriedenheit, was der Net Promoter Score mit einem durchschnittlichen Wert von 90 in den vergangenen sieben Jahren beweist.

Nutanix arbeitet in Deutschland und weltweit mit starken Partnern zusammen. Dazu zählen im öffentlichen Sektor, aber auch speziell im Bereich der kritischen Infrastrukturen bekannte Lieferanten wie Dell, Fujitsu oder HPE sowie Dienstleister und Distributoren.

KRITIS-RECHENZENTREN: VORREITER DER DIGITALISIERUNG IN DEUTSCHLAND

Die Softwaresteuerung von Nutanix ermöglicht und beschleunigt nicht nur die Standardisierung in öffentlichen Rechenzentren. Vielmehr leistet sie auch einen entscheidenden Beitrag dazu, die damit verbundenen Ziele von Wirtschaftlichkeit und Effizienz über Skalierbarkeit, Sicherheit und Interoperabilität bis hin zu Offenheit und Agilität zu erreichen. Mithilfe der hyperkonvergenten Infrastruktursoftware von Nutanix werden KRITIS-Rechenzentren zum Vorreiter der Digitalisierung in Deutschland.

TESTEN SIE UNS!

Probieren geht über studieren – das gilt auch und gerade für hyperkonvergente Infrastruktursoftware. Testen Sie uns und unser Angebot. Nutzen Sie online unsere Testumgebung „Nutanix Test Drive“ und erleben Sie live die Leistungsfähigkeit und Funktionsweise unserer Software. Zögern Sie nicht. Melden Sie sich an.

TEST DRIVE!

Als führender Anbieter von Cloud-Software und Pionier im Bereich hyperkonvergenter Infrastrukturlösungen macht Nutanix Computing überall unsichtbar. Kunden weltweit profitieren von der Software des Anbieters, um von einer zentralen Plattform aus jede App an jedem Ort – in privaten und hybriden wie in Multi-Cloud-Umgebungen – zu managen und beliebig zu skalieren. Weitere Informationen sind auf www.nutanix.de oder über Twitter unter @NutanixGermany erhältlich.

NUTANIX™
Your Enterprise Cloud Platform

info@nutanix.com | www.nutanix.com | @nutanix

Stand: Oktober 2021