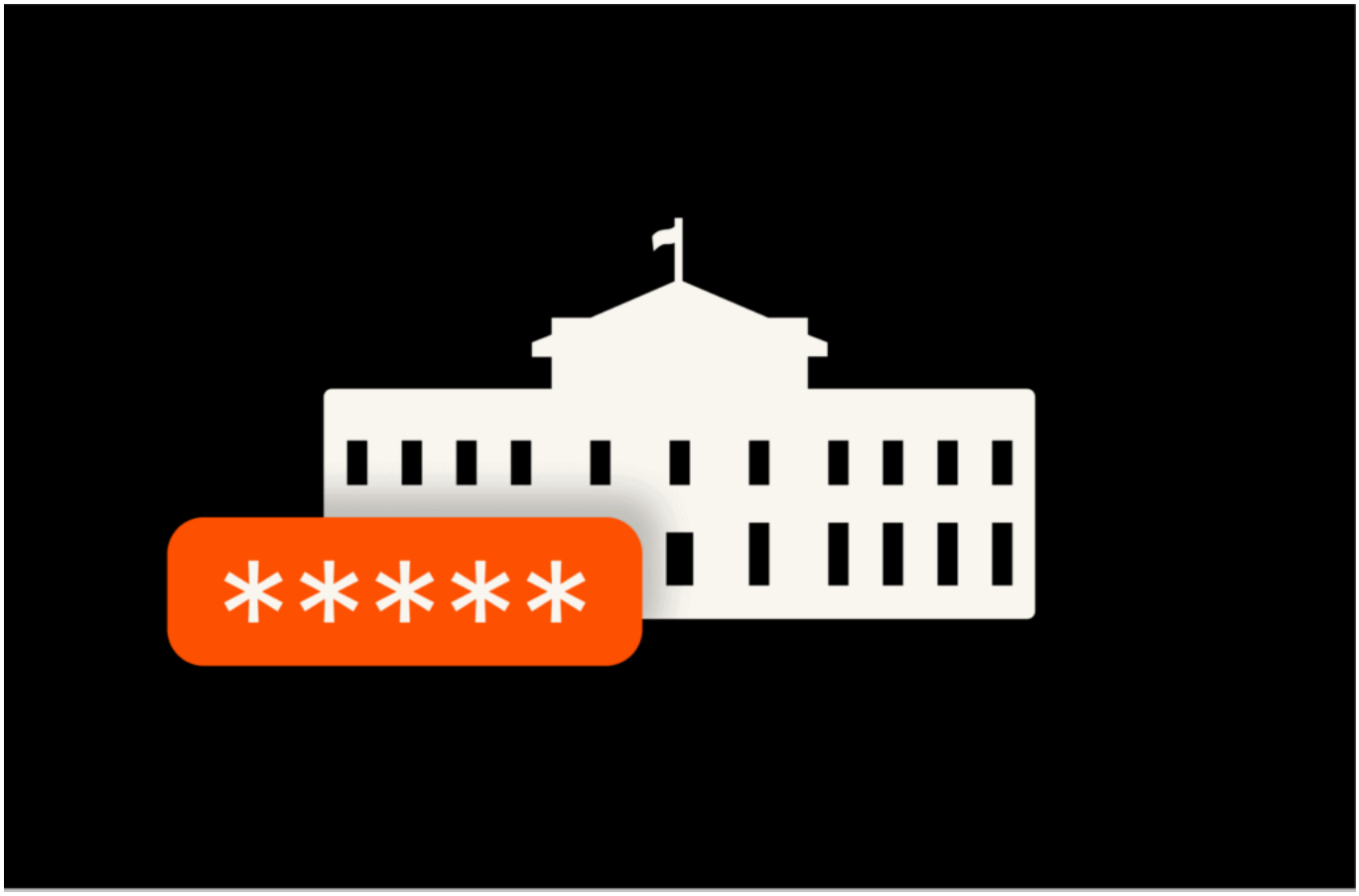
De nieuwste nationale cyberbeveiligingsrichtlijn: Wat beveiligingsteams moeten weten



De National Cybersecurity Strategy (NCS) is meer dan alleen maar een set cyberrichtlijnen – het is een wake-up call. Cyberbedreigingen nemen toe en natiestaten en criminelen richten zich op kritieke infrastructuur en bedrijven als nooit tevoren. Dit zijn geen theoretische risico's. Ze gebeuren nu.

De strategie zet de toon voor hoe de federale overheid van ondernemingen verwacht dat zij zich opvoeren: Neem veilige softwarepraktijken aan, verscherp de beveiliging van de toeleveringsketen en bereid u voor op opkomende bedreigingen. Als uw onderneming niet op één lijn zit met deze verwachtingen, bent u niet alleen kwetsbaar voor aanvallen – u loopt het risico achter te raken in

een landschap waar cyberbeveiliging niet langer optioneel is, maar ook een zakelijke noodzaak. Laten we hieronder eens kijken naar de nieuwste cyberbeveiligingsrichtlijnen en hoe zowel federale instanties als de particuliere sector veerkrachtig en klaar kunnen blijven. Het is belangrijk om in gedachten te houden dat hoewel veel van deze richtlijnen vanuit technologisch perspectief toekomstgericht zijn, NU het moment is om aan de slag te gaan en een plan te bedenken om ze op langere termijn aan te pakken.

Wat is er nieuw in 2025: Versterking en bevordering van innovatie in de cyberbeveiliging van het land

Op 16 januari 2025 heeft president Joe Biden een Executive Order uitgevaardigd die gericht is op het versterken van de cyberbeveiligingsverdediging van het land, het aanpakken van onderwerpen zoals AI, open-source softwareproblemen, kwantumcomputing, IoT-beveiliging, bedreigingen van identiteitsdiefstal (identiteit *is* de nieuwe netwerkbeveiligingsperimeter) en aanvallen gericht op kritieke infrastructuur. Over het algemeen volgt de richtlijn een paar belangrijke beloften in de NCS van vorig jaar op, waaronder:

- **Verbeterde normen voor federale aannemers:** Strenge cyberbeveiligingsnormen voor overheidstechnologiecontractanten vereisen dat zij verifieerbaar bewijs leveren van naleving van veilige softwareontwikkelingspraktijken.
- **Verantwoordelijkheid voor de toeleveringsketens van software van derden:** Om kwetsbaarheden te beperken die kritieke federale systemen bedreigen, moeten softwareproviders attesten en artefacten indienen die aantonen dat ze voldoen aan veilige ontwikkelingspraktijken. Deze inzendingen, gevalideerd via CISA's Repository for Software Attestation and Artifacts, zullen providers verantwoordelijk houden voor het aanpakken van bekende kwetsbaarheden, met de nadruk op beoordelingen, patching en veilige bijdragen.
- **Versnelde gevolgen voor buitenlandse cyberbedreigingsdaders:** De

richtlijn breidt de bevoegdheid uit om sancties op te leggen aan buitenlandse personen en entiteiten die zich bezighouden met cyberaanvallen tegen de VS, met een bijzondere focus op ransomware-aanvallen die zich richten op kritieke infrastructuur zoals gezondheidszorginstellingen.

- **Een blik op kwantumbestendige beveiligingsmaatregelen:** Federale instanties zullen de overgang naar kwantumbestendige cryptografische algoritmen moeten versnellen om gevoelige data te beschermen tegen toekomstige bedreigingen door de vooruitgang in de decryptie van kwantumcomputing.
- **Integratie van artificiële intelligentie in cyberverdediging:** De richtlijn bevordert het gebruik van op kunstmatige intelligentie gebaseerde tools om de federale cyberbeveiligingsinspanningen te verbeteren. Nieuwe AI-programma's binnen afdelingen zoals het Pentagon om cyberverdedigingsmechanismen te versterken, omvatten pilotprogramma's in kritieke sectoren zoals energie.
- **Een nieuw Cyber Trust Mark-programma voor IoT:** Het bevel kondigt de ontwikkeling aan van het Cyber Trust Mark-programma, geplaagd in de National Cybersecurity Strategy van vorig jaar, ontworpen om de veiligheid van slimme apparaten te certificeren om de bescherming voor zowel federale instanties als de particuliere sector te verbeteren.

De nationale cyberbeveiligingsstrategie van 2024

De NCS die in juni 2024 is bijgewerkt, omvat 100 federale initiatieven – een stijging ten opzichte van 69 in 2023 – met 31 nieuwe initiatieven om opkomende bedreigingen aan te pakken en "aansporingen om investeringen in cyberbeveiliging en veerkracht op lange termijn te bevorderen" opnieuw uit te lijnen. De bijgewerkte strategie is ook gericht op het versterken van kritieke infrastructuren, met een grotere nadruk op sectorspecifieke cyberbeveiligingsmaatregelen voor infrastructuren voor gezondheidszorg, onderwijs en openbare werken zoals afvalwatersystemen.

Met zoveel fronten in de strijd tegen cybercriminaliteit kan het gemakkelijk zijn om over het hoofd te zien dat de belangrijkste bijna altijd in uw eigen datacenter zal zijn. Laten we de NCS uitpakken en wat u kunt doen om de begeleiding en ondersteuning ervan te benutten.

Nieuwe bedreigingen vereisen nieuwe verdedigingen

Veel van de doelstellingen van het rapport zijn in reactie op technologieën die in verkeerde handen dubbelgekante zwaarden kunnen blijken te zijn:

- Artificiële intelligentie, met tools zoals WormGPT die alleen maar krassen op het oppervlak van wat AI in verkeerde handen zal doen.
- Quantum computing, met “het potentieel om enkele van de meest alomtegenwoordige encryptiestandaarden die vandaag de dag worden geïmplementeerd te doorbreken”. Het toekomstige doel is om “prioriteit te geven aan de overgang van kwetsbare publieke netwerken en systemen naar kwantumbestendige cryptografie-gebaseerde omgevingen en complementaire beperkingsstrategieën te ontwikkelen om cryptografische agility te bieden in het licht van onbekende toekomstige risico’s”.
- IoT-apparaten, die onderworpen zullen zijn aan een vrijwillig cyberbeveiligingslabelprogramma om het “smart grid van de toekomst” te ontwikkelen en fabrikanten aan te moedigen om te voldoen aan hogere cyberbeveiligingsnormen.
- Slimme, verbonden digitale toeleveringsketens. Eén initiatief omvat het verlenen van toegang tot en het gebruik van risicobeoordelingstools voor de toeleveringsketen, samen met professionele analytische ondersteuningsdiensten om risico’s voor de toeleveringsketen te identificeren, te beoordelen, te beperken en te monitoren.

De strategie pakt ransomware ook verder aan en belooft wereldwijde

samenwerkingen om ransomware en door de staat gesponsorde cyberspionage te ontmantelen.

Een belangrijke schijnwerper op kritieke publieke infrastructuur

De verstoring van de pijplijn van 2021 heeft ons een waardevolle les geleerd: Het afsluiten van één aanbieder van kritieke infrastructuur kan een verwoestend rimpeleffect hebben. De eerste pijler van de strategie van 2024 omvat nieuwe mandaten dat infrastructuuraanbieders moeten voldoen aan een basislijn van cyberbeveiligingsnormen, waaronder water, elektriciteitsnetten, spoorwegen en pijpleidingen.

Deze zullen afkomstig zijn van een tweede ontwikkeling van het National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), dat zal worden verfijnd en verbeterd om gelijke tred te houden met technologie en bedreigingstrends, de geleerde lessen te integreren en de beste praktijken gemeenschappelijke praktijken te maken.

Zelfs als uw organisatie niet tot de publieke sector behoort, is het een aanpak die het emuleren waard is. Dit is het moment om waakzaam te zijn en stappen te ondernemen om de digitale middelen te beschermen die het belangrijkst zijn voor uw bedrijf.

Belangrijkste pijlers en doelstellingen om op te merken

Pijler 1: Verdedig kritieke infrastructuur

Kritieke infrastructuur heeft het laatste nieuws gehaald op het gebied van cybersecurity, waaronder luchtvaart, spoor, olie en gas, afval en water, en energie, plus hun externe leveranciers. Het is een prioriteit in het NCS, waarvoor de verplichte naleving van bijgewerkte kaders van NIST, het Cybersecurity and Infrastructure Security Agency (CISA) en meer nodig is. Nauwe publiek-private

samenwerking is een primaire doelstelling van deze pijler, ontworpen om de ontwikkeling en adoptie van software en hardware te stimuleren die door ontwerp en standaard veilig is.

De prioriteiten zijn:

- Samenwerking met software-, hardware- en managed service providers om het cyberlandschap te hervormen om de veiligheid en veerkracht te versterken. Dat omvat het afdwingen van secure-by-design-principes – het ontwikkelen van producten om vanaf de basis veilig te zijn.
- Veerkracht, herstelbaarheid en beschikbaarheid/veilige failover van belangrijke systemen en diensten in deze sector – iets dat kan worden bereikt met een gelaagde back-uparchitectuur. (Meer hierover hieronder.)
- Naleving van alle externe leveranciers. U bent slechts zo veilig als uw zwakste schakel.

Lees meer: Hoe zet u de aanbevelingen van CISA 'Shields Up' in actie

Pijler 2: Dreigingsacteurs verstoren en ontmantelen

De overheid heeft beloofd "alle instrumenten van nationale macht" te gebruiken, met inbegrip van tegengestelde takedown- en disruptiecampagnes die gericht zijn op kwaadwillende actoren. De strategie roept specifiek op:

- Bedrijven ontmoedigen om losgeld te betalen – wat vereist dat u een veerkrachtige architectuur hebt met veilige back-ups als onderdeel om het betalen van losgeld een moot point te maken
- Verbeterde bidirectionele uitwisseling van informatie – waarbij CISA waarschuwingen kan delen en particuliere organisaties middelen kan geven om geclassificeerde bedreigingen te delen via "hubs" voor meer georganiseerde rapportage-inspanningen

Dit is bemoedigend, maar organisaties zelf moeten ook aan het offensief blijven, niet alleen aan het verdedigende. Dit komt voort uit het weten wie aanvallers zijn en wat ze zoeken en ook volledig inzicht hebben in een data estate met geavanceerde anomaliedetectie. Om uw steentje bij te dragen, wilt u snelle, nauwkeurige, toegankelijke beveiligingslogboeken, SIEM met krachtige onderliggende opslagtechnologieën zodat opname nooit een knelpunt is, en back-upplannen voor het forensische proces.

Pijler 3: Marktkrachten vormgeven om veiligheid en veerkracht te stimuleren

Een belangrijk thema in de strategie is het verminderen van de onus op individuen en kleine bedrijven, omdat het aanvalsoppervlak blijft uitbreiden met externe leveranciers en software-as-a-service. Het afdwingen van meer en betere beleidslijnen voor datanaleving en -privacy zal helpen om “verkopers van software en hardware aansprakelijk te stellen als ze geen erkende beveiligingsontwikkelingspraktijken toepassen”.

Om veiligheid en veerkracht te stimuleren, wil de NCS organisaties meer verantwoordelijk houden voor databeveiliging door het afdwingen van:

- Bescherming van gevoelige persoonsgegevens door het verzamelen en gebruiken te beperken. Het is een goed moment om uw best practices op het gebied van compliance te controleren.
- Aansprakelijkheid voor kwetsbaarheden in software
- Vereiste naleving van federale leveranciers (bijv. FIPS of SOC 2 Type II)

Het “backstop”-fonds voor cyberverzekeringen om te helpen bij catastrofale beveiligingsgebeurtenissen blijft een strategische doelstelling onder deze pijler.

Pijler 4: Investeer in een veerkrachtige toekomst

Het is de vierde pijler, maar naar mijn mening de belangrijkste – en de meest

bruikbare. Het federale doel is om “[lead]de wereld te beschermen tegen veerkrachtige technologieën en infrastructuur van de volgende generatie door middel van strategische investeringen en gecoördineerde, collaboratieve actie”. Dit omvat nieuwe initiatieven om de gaten in de beveiliging van Border Gateway Protocol (BGP) en Internet Protocol versie 6 (IPv6) aan te pakken. Volgens de strategie betekent investeren in veerkracht:

- Het verminderen van kwetsbaarheden in fundamentele technologie, waaronder kritieke infrastructuur zoals opslag, die in staat moet zijn tot gelaagde back-ups, SLA-gebaseerde herstelgaranties, onveranderlijke snapshots en snelle hersteltijden.
- Versterking en beveiliging van het open-source software-ecosysteem om kwetsbaarheden van externe softwareleveranciers te verminderen.
- Digitale identiteitsoplossingen met de “juiste” controles om compromissen van niet-menselijke identiteiten en accounts te beperken of te voorkomen.
- Het implementeren van een schone energie-infrastructuur om nog een laag veerkracht in te bouwen door de energiekosten en -uitval te verhogen – in overeenstemming met de decarbonisatiedoelstellingen van de overheid. Dit begint in het datacenter.
- Quantum-resistente cryptografie met post-kwantum algoritmen.

Dit komt neer op één kritisch concept: **een gelaagde veerkrachtarchitectuur.** Een veerkrachtarchitectuur kan uw gehele data estate beschermen, wat ik in dit artikel heb beschreven. Het is de beste manier om elke kans te hebben om te herstellen na een beveiligingsincident.

Pijler 5: Internationale partnerschappen aangaan om gedeelde doelen na te streven

Samenwerking en communicatie zijn van vitaal belang om aanvalsgebieden te verkleinen, bedreigingen tegen te gaan, wereldwijde toeleveringsketens te beveiligen en elkaar na een aanval te ondersteunen. De National

Telecommunications and Information Administration heeft meer dan 140 miljoen dollar geïnvesteerd uit het Public Wireless Supply Chain Innovation Fund om de veerkracht van de wereldwijde toeleveringsketen te helpen versterken en de kosten voor consumenten en netwerkoperators te verlagen.

Hoewel de overheid werkt aan het bevorderen van “verantwoord staatsgedrag” en bondgenoten hun beste beeld geeft van cyberbeveiligingsveerkracht, blijft het feit dat organisaties een doelwit zullen zijn zolang ze in bedrijf zijn. Voor u betekent dit dat u zorgvuldig moet blijven en zich moet voorbereiden op een worst-case scenario. Bij Pure Storage helpen we klanten niet alleen om zich voor te bereiden op het ergste, maar ook om er in recordtijd van te herstellen.

Hoe kunt u er klaar voor zijn? Bewezen, gelaagde cyberveerkracht op het Pure Storage-dataplatform

Bij Pure Storage delen we deze prioriteiten en innoveren en evolueren we voortdurend om onze klanten op de hoogte te houden van cyberveerkracht en -beveiliging. Onze onlangs aangekondigde SLA’s en AI-gestuurde beveiligings- en cyberveerkrachtsmogelijkheden geven onze klanten een duidelijk voordeel in de voortdurende oorlog tegen cybercriminaliteit.

Waar te beginnen? De meest effectieve manier om veerkrachtig te blijven is met **een gelaagde veerkrachtarchitectuur** die is gebouwd op een uniform dataplatform zoals Pure Storage. Dit kan uw bedrijf in enkele minuten versus uren of dagen laten herstellen.

1. **Tier 1: Primaire, bedrijfskritische data en veilige back-ups.** Sla applicaties op die cruciaal zijn voor activiteiten en drie tot zeven dagen SafeMode™ Snapshots.
2. **Tier 2: Betaalbare second-tier data, snapshotarchieven en forensische data.** Behoud geoffloade Tier 1-snapshots betaalbaar (bij voorkeur 6-12 maanden) en data die nodig zijn voor forensisch onderzoek na een aanval, en bewaar een replica-archief voor opslag op “langere termijn” (6-12 maanden – of langer, indien mogelijk).

3. **Tier 3: Snelle back-uplaag.** Dit niveau is voor extreme scenario's en langdurige retentie voor compliance of applicaties die geen snapshots rechtvaardigen.
4. **Tier 4: Een eenrichtingsdatabunker.** Voor grootschalige rampen zijn databunkers zeer veilig en bieden ze extra, optionele disaster recovery-locaties achter primaire en secundaire back-uplocaties. U kunt jarenlange data opslaan op de Tier 4-laag.

Zelfs nog is het een kwestie van wanneer, niet als. Ontdek meer over onze onlangs bijgewerkte SLA voor cyber recovery in Evergreen//One™, die de volgende werkdag verzending van clean recovery array(s)* omvat, zodat u een schone omgeving hebt om naar te herstellen na een cybergebeurtenis.

We spelen allemaal een belangrijke rol in de strijd tegen cybercriminelen. Pure Storage biedt de ultieme gemoedsrust in dit evoluerende landschap.

****Verzendschema: Verzending van arrays naar Noord-Amerika en EMEA op de volgende werkdag. Drie werkdagen naar Azië en Australië/Nieuw-Zeeland. Versnelde verzending kan beschikbaar zijn, afhankelijk van de regio.***