

De toekomst veiligstellen: een gesprek met Jen Easterly over cyberdreigingen, vertrouwen en leiderschap in een digitale wereld

15 mei 2025, 10:24

Ann Debaere

In een wereld waar ontwrichting onvermijdelijk is, is veerkracht niet optioneel, maar essentieel. Weinig leiders begrijpen dit beter dan Jen Easterly, voormalig directeur van het Amerikaanse Cybersecurity and Infrastructure Security Agency (CISA) en gedecoreerd legerofficier. In de aanloop naar haar keynote op Securing Tomorrow. Now., het jaarlijkse evenement van Agoria & Sirris op woensdag 4 juni in de Skyhall (Brussels Airport), spraken we met Easterly over leiderschap, cyberweerbaarheid, de rol van Europa in de wereldwijde beveiliging en hoe bedrijven zich moeten aanpassen aan een volatiele digitale toekomst.

Welke lessen over veerkracht hebt u geleerd bij het leger en de inlichtingendienst en zijn ook rechtstreeks van toepassing op bedrijfsleiders?

Jen Easterly: Een van de belangrijkste lessen is dat veerkracht niet alleen gaat over terugveren, maar ook over ‘vooruit veren’. Het gaat erom schokken beter op te vangen, je onder druk aan te

passen en er sterker uit te komen.

Daar is meer voor nodig dan voorbereiding alleen. Het vergt leiderschap, vertrouwen en een sterke cultuur. Het is onmogelijk om elke ontwrichting te voorkomen. Veerkracht impliceert dat u die realiteit aanvaardt en zich voorbereidt om doelgericht te reageren en te recupereren dankzij getrainde teams, veerkrachtige systemen en een duidelijke missiementaliteit.

Wat denkt u over de inspanningen die Europa levert om de hui



Jen Easterly, Former Director, U.S. Cybersecurity and Infrastructure Secure Agency

Jen Easterly: Cyberspace kent geen grenzen en Europa heeft belangrijke stappen gezet op het gebied van privacywetgeving en een geharmoniseerd cyberbeleid. Het dreigingslandschap verandert echter sneller dan het beleid of de bureaucratieën kunnen bijhouden.
We hebben snelheid, durf en samenwerking nodig, vooral grensoverschrijdende partnerschappen tussen overheid en privésector. Cyberdreigingen zijn wereldwijd, dus onze verdediging moet dat ook zijn.

Zijn er dreigingsscenario's die nog steeds worden onderschat door de leiders, vooral in Europa?

Jen Easterly: Ja, vooral de strategische dreigingen op lange termijn van natiestaten zoals China en Rusland. Cybercriminelen zijn gevaarlijk, maar staatsactoren vormen een nog groter risico. In de VS hebben we gezien dat Chinese actoren de kritieke infrastructuursectoren infiltreren.
Ook kunstmatige intelligentie is een belangrijke risicovector die geavanceerdere cyberaanvallen, deepfakes en desinformatie mogelijk maakt. Deze risico's zijn niet theoretisch; ze doen zich nu al voor.

Als directeur van CISA hebt u een grote transformatie geleid. Hoe hebt u het agentschap gemoderniseerd?

Jen Easterly: Toen ik bij CISA aan de slag ging, waren we een jong bureau met een enorm personeelstekort: er waren ongeveer 1.000 vacatures. We moesten snel capaciteit en bekwaamheid opbouwen.
Daartoe hebben we aanwervingsprocessen gestroomlijnd, en een ware culturele transformatie doorgevoerd. We creëerden een missiegedreven, mensgerichte cultuur die technisch toptalent en samenwerkingstalent kon aantrekken. Vertrouwen – zowel intern als met de partners – was van fundamenteel belang.

Welke concrete maatregel hebt u genomen om toptalent aan te trekken en te behouden?

Jen Easterly: Tijdens mijn ambtstermijn hebben we meer dan 2.200 mensen aangenomen, niet alleen technische experts, maar ook mensen die konden samenwerken. We bouwden actief aan een werkplek waar mensen zich gesterkt en gewaardeerd voelden en werden verenigd door een hoger doel. En die cultuur maakte het verschil in een concurrentiële markt.

De belangrijkste citaten van Jen Easterly

- “Veerkracht is niet alleen terugveren, maar ook ‘vooruit veren’.”
- “Je maakt geen vrienden tijdens een crisis. Vertrouwen moet van tevoren worden opgebouwd.”
- “Op het vlak van cyberbeveiliging moeten we leveranciers verantwoordelijk stellen in plaats van schurken te verheerlijken.”
- “De verantwoordelijkheid voor beveiliging mag niet op de schouders van gebruikers rusten. Ze moet integraal deel uitmaken van het design.”
- “De toekomst behoort toe aan mensen die dapper genoeg zijn om ze vorm te geven. Morgen veiligstellen begint vandaag.”
- “Goede cyberhygiëne kan tot 98 procent van de aanvallen voorkomen. De fundamenten zijn het belangrijkst.”

Welke realisaties van CISA, zoals het Joint Cyber Defense Collaborative, kunnen worden toegepast in België of Europa?

Jen Easterly: We hebben het Joint Cyber Defense Collaborative (JCDC) opgericht om de afscheiding tussen inlichtingen-, wetshandhavings- en cyberdefensie-instanties te doorbreken en rechtstreeks met de privésector samen te werken.

Deze realtime, operationele samenwerking bleek van vitaal belang bij crises zoals de Log4j-kwetsbaarheid en de Russische invasie in Oekraïne. Canada heeft sindsdien zijn eigen versie gemaakt. Ik denk dat Europa baat zou hebben bij een soortgelijk model, niet alleen op nationaal

niveau, maar in de hele EU.

Zoals ik vaak zeg: je maakt geen vrienden tijdens een crisis. Vertrouwen en samenwerking moeten van tevoren worden opgebouwd.

Hoe moet de internationale samenwerking zich ontwikkelen om het grensoverschrijdende karakter van cyberdreigingen aan te kunnen?

Jen Easterly: We hebben realtime operationele samenwerking nodig, niet alleen allianties op papier. In de VS is cyberbeveiliging verheven tot een nationale veiligheidskwestie met een ernstige leiderschapsfocus en financiering.
Europa heeft veel sterktes, maar zou baat hebben bij een meer verenigde aanwending van de nationale capaciteiten. Een geïntegreerde EU-aanpak, met sterke banden met de VS en bondgenoten, zal cruciaal zijn om de toekomstige cyberdefensie het hoofd te bieden.

U bent een uitgesproken voorstander van de 'Secure by Design'-beweging. Wat moeten digitale bedrijven anders doen?



Jen Easterly: We verheerlijken schurken zoals Volt Typhoon en geven slachtoffers de schuld omdat ze hun systemen niet patchen, terwijl we eigenlijk de technologieleveranciers verantwoordelijk moeten stellen.
Beveiliging moet een kernaspect van het design zijn, waaraan CEO's, directies en productteams vanaf dag één prioriteit geven. Snelle marktlanceringen en kostenbesparingen krijgen vaak voorrang op beveiliging en dat moet veranderen.
Sinds we onze ‘Secure by Design’-belofte hebben gelanceerd, werd deze al door meer dan 300 bedrijven ondertekend. Europa loopt voorop met initiatieven zoals de Cyber Resilience Act, waarmee de EU sneller dan de VS strengere beveiligingsnormen oplegt.
U zou vandaag toch ook geen auto zonder veiligheidsgordels meer kopen? In dezelfde optiek zouden we niet mogen aanvaarden dat digitale producten geen ingebouwde basisbescherming bieden.

Hoe kunnen productiebedrijven een beter evenwicht vinden tussen innovatie en cyberbeveiliging?

Jen Easterly: Innovatie is essentieel, maar beveiliging moet vanaf het begin worden ingebouwd. Productiebedrijven moeten inzicht hebben in hun 'kroonjuwelen' – hun kritieke systemen en gegevens – zodat ze deze kunnen beschermen met een gelaagde verdediging en netwerksegmentatie.
Cyberbeveiliging wordt nog al te vaak als een verzekeringspolis gezien, terwijl het eigenlijk als een kerninvestering moet worden behandeld, net als innovatie en productiviteit. Bedrijven moeten hun koopkracht gebruiken om een betere beveiliging te eisen van hun leveranciers.

Wat zijn de drie prioriteiten inzake cyberbeveiliging voor kleinere ondernemingen die niet over de middelen van grote bedrijven beschikken?

Jen Easterly:

1. **Installeer updates**: veel aanvallen maken gebruik van bekende kwetsbaarheden die door updates zouden worden verholpen.
2. **Gebruik sterke wachtwoorden en een wachtwoordmanager**: unieke wachtwoorden zijn van cruciaal belang.
3. **Denk na voordat u klikt**: leid werknemers op om op hun hoede te zijn met e-mails, sms'jes en telefoontjes.

Schakel ook multifactorauthenticatie (MFA) in. Deze basisstappen – of cyberhygiëne – kunnen tot 98 procent van de aanvallen voorkomen.

Welke concrete stappen kunnen leiders zetten om cyberbeveiliging in hun organisaties te verankeren?

Jen Easterly:

- **Maak het persoonlijk**: verbind acties met echte risico's door verhalen te vertellen, niet door angst aan te jagen.
- **Leid van bovenaf**: CEO's en raden van bestuur moeten cyberbeveiliging behandelen als een leiderschapsverantwoordelijkheid, niet als een IT-probleem.
- **Vier beveiliging**: erken en beloon veilige praktijken in de hele organisatie.

Er moet een cultuurwijziging komen en die begint bij leiders die niet alleen hun mond opentrekken maar ook de daad bij het woord voegen.

Tot slot, waarom moeten Belgische bedrijfsleiders 'Securing Tomorrow. Now.' bijwonen en uw keynote beluisteren?

Jen Easterly: Omdat de toekomst vandaag wordt geschreven, en omdat ze toebehoort aan mensen die dapper genoeg zijn om ze vorm te geven. De dreigingen zijn urgent, maar de kans om een veiligere, sterkere digitale wereld op te bouwen is dat ook.

In Brussel zal ik lessen uit de frontlinie delen over leiderschap, veerkracht en het veiligstellen van onze toekomst. Ik kom niet alleen om te informeren, maar ook om te inspireren.

Auteurs



Ann Debaere