Cyberbezpieczny samorząd – kompleksowa ochrona

Monitoruj wykorzystanie internetu i chroń samorząd przed atakami DDoS

Zarządzany UTM

Jak dbać o bezpieczeństwo:

Zabezpiecz sieć przed cyberzagrożeniami.
Monitoruj wykorzystanie internetu
i określaj reguły dostępu do stron WWW.

Dlaczego?

Aby kompleksowo zabezpieczać
jednostki samorządowe

Rozwiązania od Orange:

- Zarządzany UTM – nie wymaga łącza OPL

Orange Internet Protection + Orange Network Security

(usługi dostępne na łączu Orange Polska)

Jak się chronić:

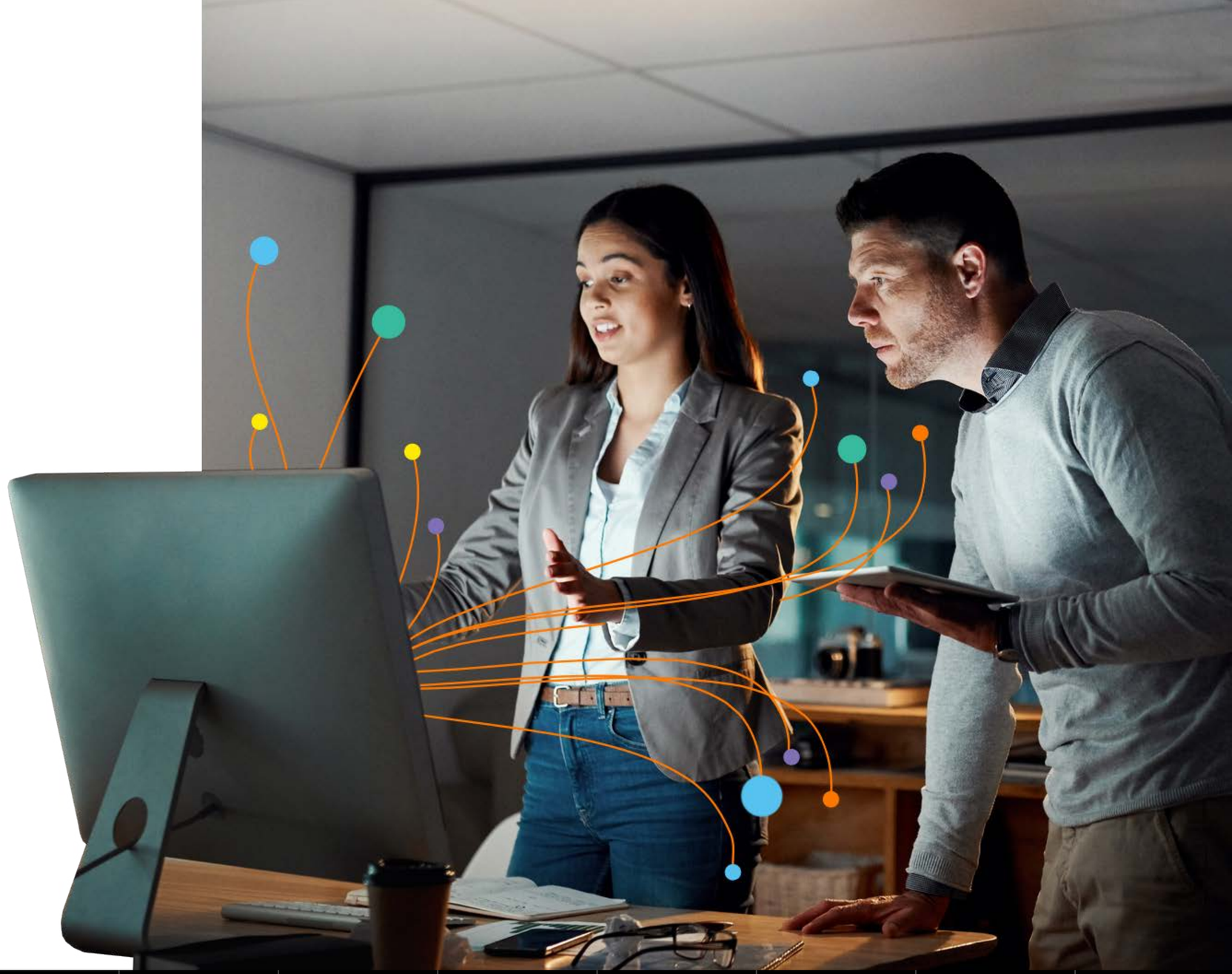
Stosuj ochronę przed atakami DDoS. Monitoruj wykorzystanie internetu i określaj reguły dostępu do stron WWW.

Dlaczego?

Aby zapewnić nieprzerwane działanie usług internetowych oraz ochronę łącza przed cyberzagrożeniami.

Rozwiązania od Orange:

- Orange Network Security
- Orange Internet Protection (usługi dostępne na łączu Orange)



SOC Lite,
Next Generation Security Operations Center

(usługi dostępne na łączu Orange Polska)

Jak się chronić:

Monitoruj incydenty bezpieczeństwa

Dlaczego?

W celu wykrywania prób kradzieży wrażliwych danych mieszkańców i/lub pracowników samorządu

Rozwiązania od Orange:

- SOC Lite, Next Generation SOC (usługi dostępne na łączu Orange)

Testy socjotechniczne, szkolenia świadomości

Jak się chronić:

Cyklicznie edukuj pracowników w zakresie podnoszenia świadomości cyberbezpieczeństwa.

Dlaczego?

Aby zwiększać odpowiedzialność i czujność pracowników oraz poszerzać ich wiedzę.

Rozwiązania od Orange:

- Testy socjotechniczne (phishingowe)
- Szkolenia podnoszące świadomość pracowników
- Szkolenia specjalistyczne z zakresu technologii
- Szkolenia z bezpieczeństwa

Testy podatności, testy penetracyjne, audyty, Cyber Pakiet

Jak się chronić:

Cyklicznie testuj poziom zabezpieczeń w ramach całego swojego biznesu (dostęp do danych, systemy, aplikacje).

Dlaczego?

Aby utrzymywać biznesowo uzasadniony poziom zabezpieczeń w JST.

Rozwiązania od Orange:

- Testy podatności
- Testy penetracyjne
- Audyty
- Cyber Pakiet

Ochrona urządzeń i użytkowników

Jak się chronić:

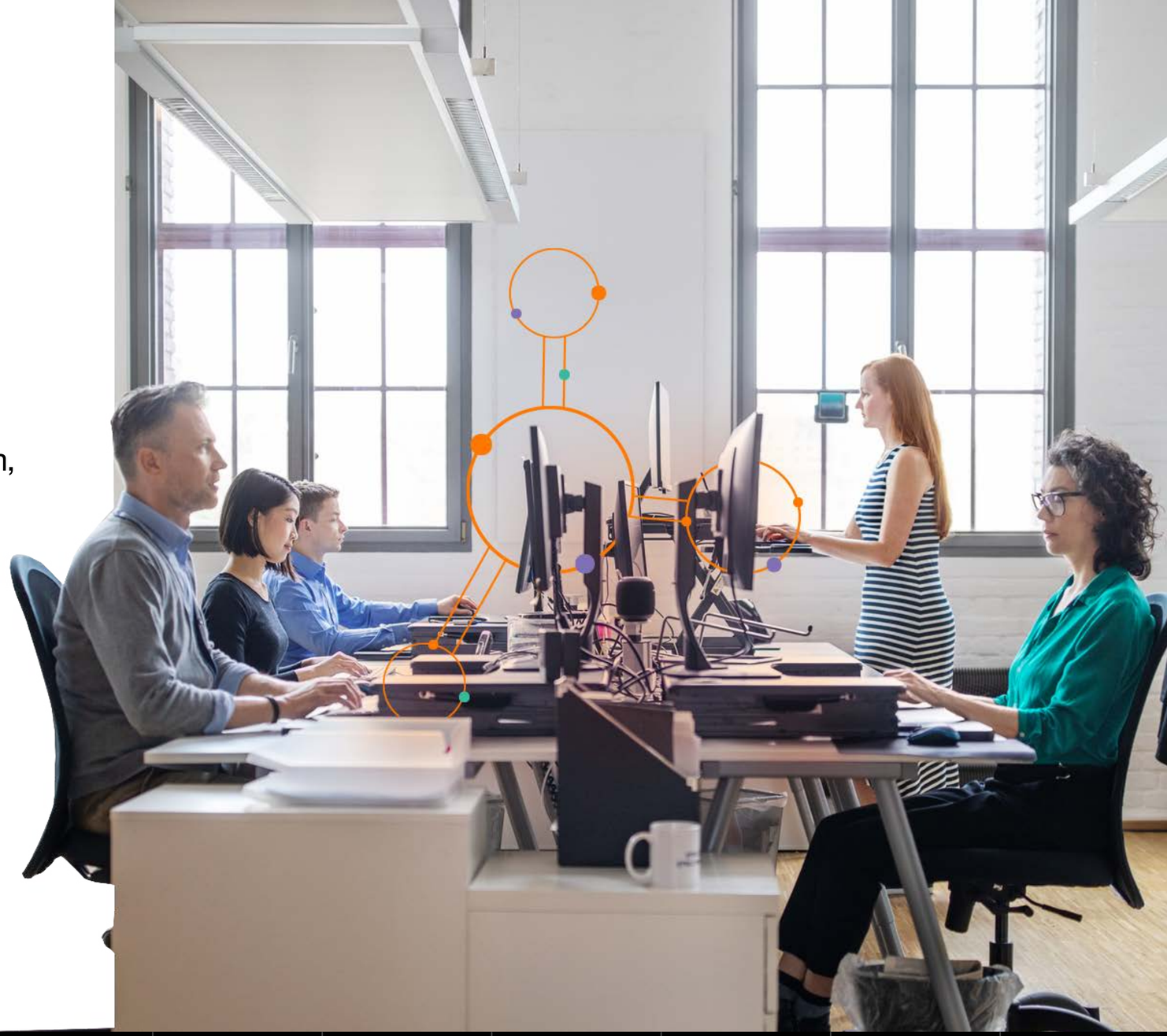
Chroń komputery pracowników, infrastrukturę techniczną, urządzenia przenośne.

Dlaczego?

Aby chronić firmę przed malware, ransomware, phishingiem, kradzieżą tożsamości.

Rozwiązania od Orange:

- Eset
- Check Point Harmony



Mobile Devices Management

Jak się chronić:

Efektywnie zarządzaj flotą urządzeń mobilnych oraz komputerów przenośnych.

Dlaczego?

Aby wzmocnić ochronę dostępu do danych, zapewnić standaryzację używanych aplikacji.

Rozwiązania od Orange:

- MDM

Integrated Computing Standard

Jak się chronić:

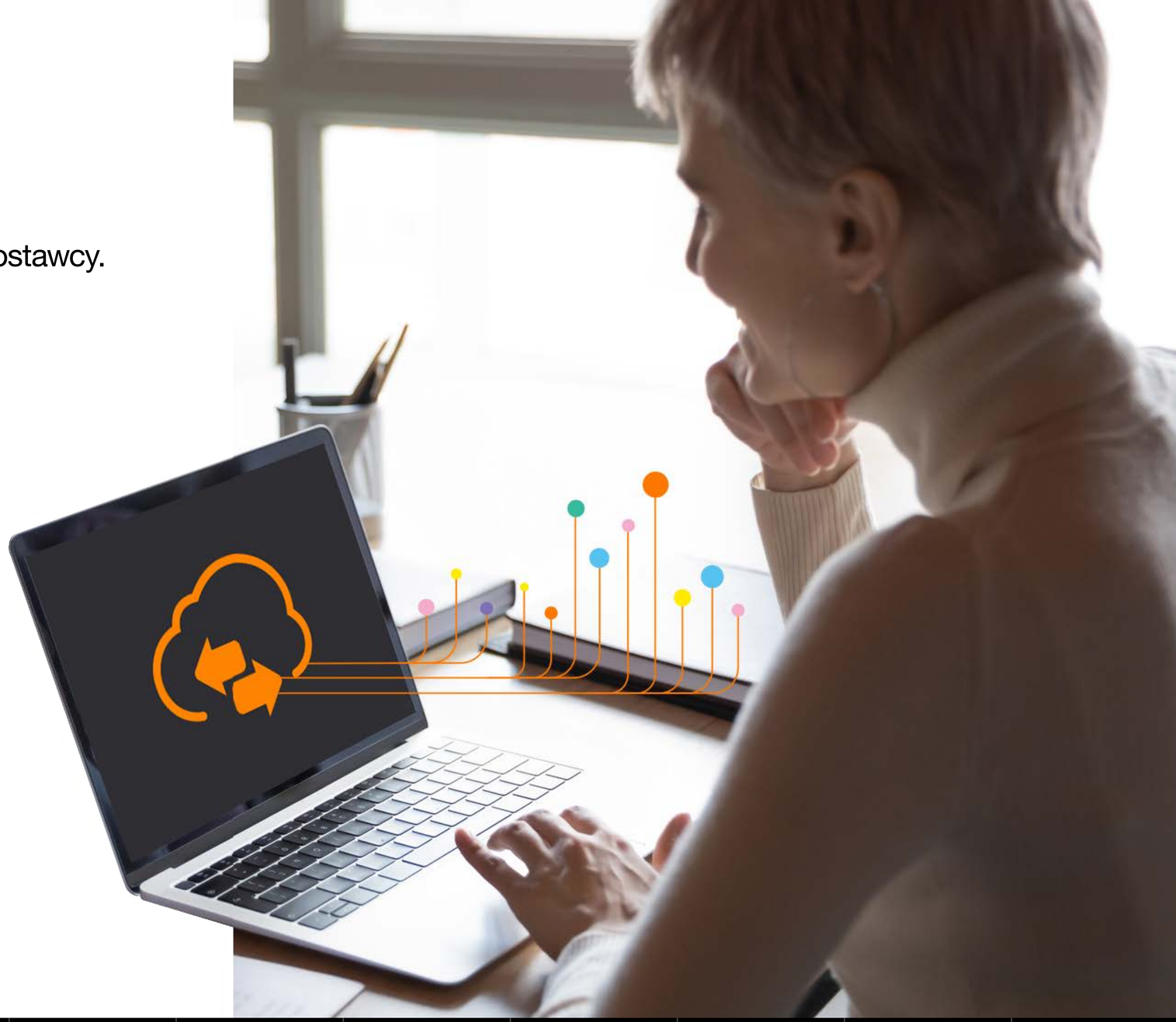
Przechowuj dane w bezpiecznym miejscu u zaufanego dostawcy.

Dlaczego?

Aby zapewnić ciągłość działania usług
oraz bezpieczeństwo swoich danych.

Rozwiązania od Orange:

- Integrated Computing Standard
  (bezpieczna chmura zlokalizowana w Polsce)



Laptopy

Jak się chronić:

Pracuj na bezpiecznym i niezawodnym sprzęcie oraz aktualnym oprogramowaniu Windows 11 Pro z możliwością szyfrowania Bitlocker.

Dlaczego?

Aby zapewnić bezpieczeństwo swoich danych oraz ograniczyć ryzyko awarii sprzętowej.

Rozwiązania od Orange:

- Laptopy i komputery wiodących producentów

Infrastruktura IT

Jak się chronić:

Przechowuj i przetwarzaj dane na niezawodnym sprzęcie IT.

Dlaczego?

Aby ograniczyć ryzyko awarii sprzętowej oraz zapewnić bezpieczeństwo swoich danych.

Rozwiązania od Orange:

- Serwery, macierze, etc. wiodących producentów

- Oferujemy nie tylko wymienione usługi i produkty, ale też dopasowane do potrzeb klienta wdrożenie.
- Możliwość zakupu produktów i usług w modelu jednorazowym i abonamentowym.
- Pracujemy z zaufanymi partnerami IT wskazanymi przez Orange lub klienta.