ECOWAS COMMISSION
COMMISSION DE LA CEDEAO
COMISSÃO DA CEDEAO

cooperation germany – ecowas

EUROPEAN UNION

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Global Gateway

SHADOWSERVER

Região da CEDEAO:

Informações e recomendações sobre cibersegurança

O desafio:

O cibercrime está a aumentar em toda a África.

Na África Ocidental, o cibercrime é responsável por mais de 30 por cento de todo o crime reportado.

Os Estados-membros da CEDEAO sofreram recentemente ciberataques onerosos e devastadores contra empresas de energia elétrica, bancos, fornecedores de telecomunicações, websites de serviços governamentais, fabricantes, entre outros.

30% DE CRIME REPORTADO na África Ocidental é cibercrime

Fatores contribuintes:

- Rápido crescimento e desenvolvimento económicos: atrai perpetradores de ataques com motivações financeiras
- Rasto digital expandido: aumenta os vetores de ataque disponíveis para invadir redes
- Falhas/"lacunas" em termos de cibersegurança: as capacidades não conseguem acompanhar as exigências

Principais ciberataques:

- Ransomware
- Ataques contra infraestruturas críticas
- Ataques de negação de serviço distribuído (DDOS)
- Comprometimento de e-mail empresarial (BEC)
- Fraudes e burlas online

Os riscos decorrentes da inação:

- Comprometer a continuidade do investimento, crescimento e desenvolvimento económicos
- Minar a confiança pública
- Impactar serviços críticos que afetam a qualidade de vida dos cidadãos

Lacunas institucionais de cibersegurança e recomendações:

Instituições eficazes

Cada Estado-Membro da CEDEAO necessita de uma CSIRT Nacional operacionalmente eficaz, acesso a um ISAC (Centro de Partilha e Análise de Informação) da CEDEAO e CSIRT Sectoriais capazes de prestar serviços de acordo com as necessidades únicas do respetivo setor.

Acesso a dados sobre ameaças, ferramentas e serviços gratuitos/acessíveis

O financiamento limitado e dados sobre ameaças, ferramentas e serviços onerosos traduzem-se pela necessidade de os especialistas em proteção beneficiarem de opções gratuitas e/ou acessíveis. Estes incluem os relatórios de remediação de redes gratuitos da Shadowserver e ferramentas como IntelMQ, Elasticsearch e Kibana necessárias para utilizar eficazmente fluxos de dados de ameaças. Existem opções comerciais acessíveis, incluindo a Arctic Hub, disponível através do Programa de Desenvolvimento de CSIRT da Arctic Security.

Formação e desenvolvimento de capacidades

Para desenvolver competências técnicas numa CSIRT ou num ISAC, os Estados-Membros devem procurar ativamente formação e projetos de desenvolvimento de capacidade financiados por ministérios governamentais, empresas do setor privado e entidades como o Banco Mundial, as Nações Unidas e a União Europeia.

Competência técnica interna

A contratação e manutenção de funcionários com competências técnicas de nível superior pode ser difícil, particularmente para entidades governamentais incapazes de competir com os salários do setor privado. Os Estados-Membros devem colaborar com as universidades e o setor privado para desenvolver programas de formação e de mentoria que possam atuar como um pipeline de talentos qualificados.

Desenvolvimento de parcerias

As CSIRT nacionais não devem trabalhar isoladamente. Devem ser concebidos quadros de referência que promovam parcerias significativas com outras CSIRT nacionais, fornecedores de serviços de Internet, operadores de infraestruturas críticas, entidades governamentais, empresas, universidades e organizações semelhantes. Esta medida facilita a partilha de informações, a colaboração e o desenvolvimento de capacidades. Estão disponíveis oportunidades de parceria por meio do FIRST.org e da comunidade online Alliance Mattermost da Shadowserver.

Lacunas institucionais de cibersegurança e recomendações:

Avaliações de maturidade

Para estabelecer um nível de maturidade inicial e monitorizar o progresso no desenvolvimento, as CSIRT Nacionais devem passar pela avaliação da ferramenta online de autoavaliação do Modelo de Maturidade de Gestão de Incidentes de Segurança (SIM3) da Open CSIRT Foundation e implementar recomendações para melhoria.

Serviços de alerta precoce

Através da utilização de relatórios diários e gratuitos de remediação de redes da Shadowserver e outros fluxos de dados sobre ameaças, as CSIRT Nacionais devem oferecer Serviços de Alerta Precoce gratuitos a todos os grupos destinatários. Estes serviços permitem que as empresas subscritoras e outros grupos de destinatários recebam notificações de alerta automáticas sobre dispositivos e serviços expostos, vulneráveis e comprometidos nas respetivas redes que necessitam de ser remediados atempadamente. A consulta com uma das inúmeras CSIRT Nacionais que oferecem Serviços de Alerta Precoce é recomendada, incluindo o Centro Nacional de Cibersegurança do Reino Unido (NCSC do Reino Unido) e o CSIRT-RD da República Dominicana.

Lacunas operacionais de cibersegurança e recomendações:

Inventários de ativos

Os proprietários de redes desconhecem muitas vezes os ativos que comprometem as suas redes. Devem ser estabelecidas políticas para mandatar a realização de inventários de ativos periódicos, em particular nos setores governamental e de infraestruturas críticas, para facilitar a remediação oportuna à medida que surgem novas vulnerabilidades.

Ativos expostos

A região contém ativos desnecessariamente expostos à Internet pública, aumentando assim as superfícies de ataques e proporcionando aos perpetradores de ataques maiores oportunidades de invasão das redes. Iniciativas focadas com CSIRT Nacionais, fornecedores de serviços de Internet e outros proprietários de redes na região poderão conduzir a atividade de reforço proativo para reduzir casos de dispositivos e serviços expostos.

Remediar vulnerabilidades críticas/de elevada gravidade

As redes da região contêm vulnerabilidades não corrigidas que podem ser exploradas por agentes de ameaças que procuram invadir essas redes e causar prejuízos através de ransomware e de outras formas de ataque. Devem ser implementados regulamentos que exijam que as agências governamentais e infraestruturas críticas remediem as vulnerabilidades designadas como “risco crítico” no prazo de 15 dias civis e as designadas como “elevado risco” no prazo de 30 dias civis a partir da data de deteção. As “vulnerabilidades exploradas conhecidas (KEV)” identificadas como ativamente exploradas em ambiente real devem receber atenção prioritária e devem ser remediadas no prazo de 14 dias civis.

Remediar dispositivos comprometidos e infetados com malware

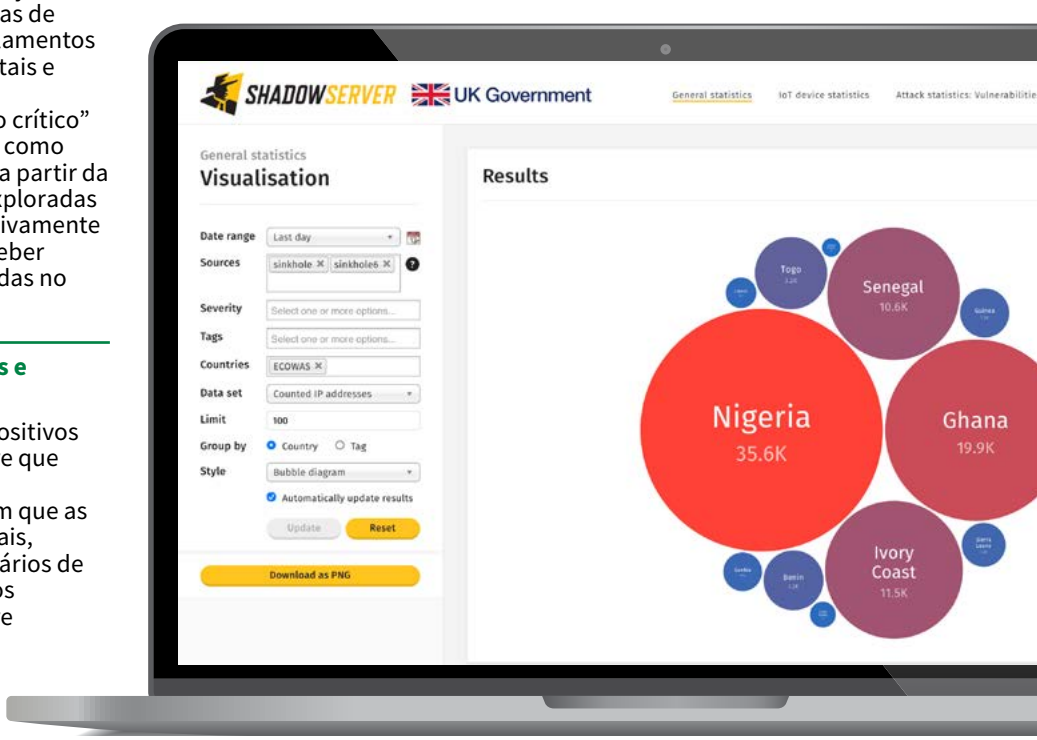
As redes da região contêm também dispositivos comprometidos e infetados com malware que necessitam de remediação. Devem ser implementados regulamentos que exijam que as CSIRT Nacionais, agências governamentais, infraestruturas críticas e outros proprietários de redes importantes remediem dispositivos comprometidos e infetados com malware identificados num período de tempo especificado, incluindo os identificados nos relatórios diários de remediação de redes gratuitos da Shadowserver disponíveis para todas as CSIRT Nacionais e proprietários de redes subscritores em todos os setores.

Campanhas de atenuação/erradicação de ameaças

Conceber e implementar campanhas de atenuação e erradicação de ameaças a nível nacional contra vulnerabilidades críticas e dispositivos comprometidos em redes espalhadas pela região. Um exemplo recente é a campanha a nível nacional liderada pela Australian Signals Directorate (ASD) para erradicar implantes em determinados dispositivos comprometidos em toda a Austrália.

Painel público da Shadowserver

Utilizar o Painel da Shadowserver como uma ferramenta para informar os principais intervenientes (por exemplo, decisores, representantes oficiais do governo, especialistas em proteção de redes, etc.) sobre as mais recentes ameaças cibernéticas que afetam a região.



Agrupamento regional de países da região da CEDEAO no Painel público da Shadowserver