SECURITY REPORT

Protegendo os ativos digitais:
Uma análise do cenário de segurança cibernética em empresas na América Latina e no Brasil

ESET Digital Security
Progress. Protected.

CONTEÚDO

INTRODUÇÃO

O **ESET Security Report** (ESR) é um relatório publicado anualmente que aborda o estado da cibersegurança corporativa na América Latina, incluindo o Brasil, e apresenta os resultados obtidos a partir de questionários respondidos por profissionais de empresas e organizações da região e informações da Telemetria da ESET. Neste contexto, não podemos esquecer que o ano de 2022 testemunhou um avanço tecnológico significativo no mundo, impulsionando a inovação e a transformação digital em diversos setores. No entanto, à medida que empresas e organizações abraçaram a digitalização para impulsionar a eficiência e a competitividade, também se tornaram alvo de ameaças cibernéticas cada vez mais sofisticadas.

Este relatório apresenta uma análise do cenário de segurança cibernética no setor corporativo do Brasil e da América Latina em 2022, reunindo dados e informações detalhadas sobre incidentes de ciberataques, vulnerabilidades exploradas e tendências emergentes, proporcionando uma visão crítica sobre os desafios enfrentados pelas empresas na proteção de seus ativos digitais.

O avanço da **Internet das Coisas** (IoT), a crescente adoção de serviços em nuvem, a expansão do e-commerce e a rápida transformação para o trabalho remoto impulsionaram a conectividade e a eficiência operacional no setor corporativo. Contudo, esse ambiente digital hiperconectado também abriu brechas para ações criminosas, resultando em consequências financeiras e reputacionais significativas para as organizações.

Este relatório não apenas alerta sobre os riscos iminentes, mas também disponibiliza recomendações e melhores práticas para que empresas e organizações possam fortalecer suas estratégias de segurança cibernética. Este documento também busca fornecer insights valiosos para que o setor corporativo possa adotar medidas proativas para combater ameaças e resguardar a confiança dos clientes e a sustentabilidade dos negócios.

DESCOBERTAS

Dois terços dos profissionais que responderam os questionários apontaram o **roubo ou vazamento de dados** como a principal preocupação em termos de cibersegurança. Em segundo lugar se destacou a preocupação com o **acesso não autorizado a sistemas;**

69% dos profissionais afirmaram ter **sofrido algum incidente de cibersegurança** no último ano;

65% dos profissionais afirmam que o **orçamento alocado para a área de cibersegurança não é suficiente;**

A adoção de soluções de segurança para dispositivos mobile, que no ano passado estava em **10%**, registrou um **aumento considerável e passou para 21%**. No entanto, ainda podemos considerar que esse é um percentual baixo em relação ao total de profissionais que responderam aos nossos questionários e a importância desses dispositivos entre usuários e o mundo corporativo;

As **detecções de vulnerabilidades bateram um recorde em 2022**, com mais de 25 mil denúncias ao longo do ano, o que representa um aumento de 26% em relação ao ano anterior;

Na América Latina, destaca-se a presença do **ransomware e trojans** que buscam roubar informações e que são distribuídos por meio de técnicas de Engenharia Social, como o spearphishing. Também o uso de outras técnicas, como extensões maliciosas para os navegadores web mais populares;

Segundo dados da Telemetria da ESET, as ameaças com o maior número de detecções no ambiente corporativo no Brasil durante 2022 estão relacionadas ao phishing; downloaders e droppers; RATs e worms; exploits; ransomware; e ameaças a dispositivos mobile.

PERCEPÇÃO DAS EMPRESAS NA AMÉRICA LATINA

PREOCUPAÇÕES

Embora as preocupações relacionadas à cibersegurança variem bastante de acordo com o tipo de organização, as informações coletadas nas pesquisas são de grande ajuda para compreender os aspectos abordados posteriormente neste relatório. Por exemplo, uma maior preocupação com o **roubo ou vazamento de informações e acesso não autorizado a sistemas** pode resultar na necessidade de implementar tecnologias de proteção e ações de capacitação. Levando isso em consideração, acreditamos que poder comparar de forma mais generalizada como as empresas na região lidam com seus incidentes e combinar essas informações com dados fornecidos pela Telemetria nas pesquisas da ESET pode ser útil para as organizações ao analisarem e avaliarem sua capacidade de detecção de ameaças e nível de autoconsciência, especialmente considerando as características dos ataques mais comuns na região e no Brasil.

Vale ressaltar que essas preocupações podem ser influenciadas por uma variedade de fatores, uma vez que cada organização possui suas particularidades, além de variar a infraestrutura tecnológica que utilizam e as medidas de proteção adotadas.

Como resultado das pesquisas realizadas com profissionais de empresas na América Latina, a principal preocupação das organizações é o **roubo/vazamento de informações** (66%), um indicador que está ligado à **perda ou destruição de informações**, identificada pelos profissionais como o ponto de maior impacto sobre as organizações.

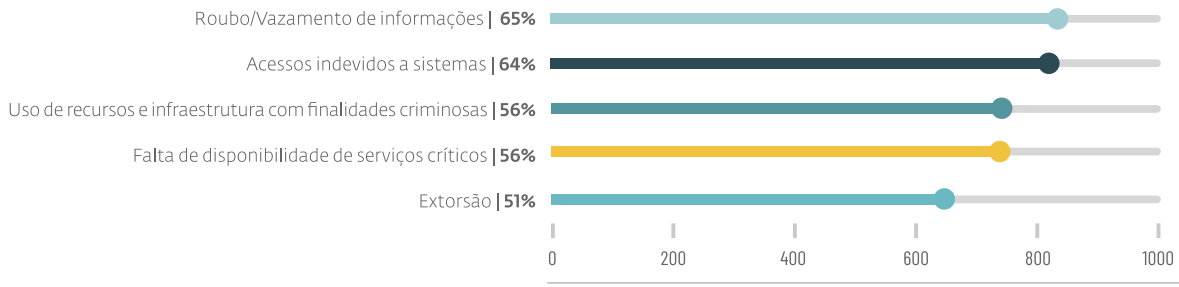

GRÁFICO 1. *PRINCIPAIS PREOCUPAÇÕES DAS EMPRESAS NA AMÉRICA LATINA EM CIBERSEGURANÇA*

Em segundo lugar, encontram-se os **acessos não autorizados a sistemas**, com **64%**. Essa preocupação, que envolve campanhas que visam realizar atividades de espionagem ou roubo de arquivos confidenciais, provavelmente está relacionada ao aumento de ataques que buscam explorar vulnerabilidades, que utilizam backdoors ou códigos maliciosos como o ransomware

e trojans de acesso remoto (RAT, pela sigla em inglês). Em terceiro lugar, no top 3 das principais preocupações, está o **de recursos e infraestrutura para fins maliciosos (56%).**

Por fim, a preocupação com a **falta de disponibilidade de serviços críticos** sofreu um leve aumento em relação à edição de 2022. Isso pode ser devido, em parte, ao retorno à presencialidade nos espaços de trabalho e à forma como as organizações redefiniram suas estratégias e arquiteturas de TI. Nesse sentido, embora 67% dos entrevistados tenham afirmado que as organizações onde trabalham estão preparadas para realizar seu trabalho de maneira híbrida, muitas organizações têm reconfigurado essa modalidade de trabalho, que apresenta diversos desafios tanto para as equipes de tecnologia quanto para as equipes de segurança.

INCIDENTES REPORTADOS

Em um mundo permeado pela tecnologia, é lógico que os incidentes de segurança que afetam os ativos de uma organização tenham consequências de alto impacto. Esses incidentes podem variar desde a interrupção da operação de serviços críticos para um país até a quebra da confiança dos clientes de uma empresa, e até mesmo a perda direta de dinheiro.

Existem várias maneiras de medir a variável de incidentes provocados, e uma delas é a consulta direta às organizações dentro da região. No entanto, não podemos esquecer que isso nos fornece apenas uma percepção subjetiva do estado da cibersegurança, já que a capacidade de detecção interna de incidentes varia entre as organizações. É inevitável que apenas uma porcentagem das tentativas de ataque que uma organização recebe seja detectada.

Essa porcentagem dependerá de vários fatores, como a complexidade dos ataques, mas principalmente das ferramentas tecnológicas, recursos humanos e práticas de gestão utilizadas internamente. Em outras palavras, uma organização tem conhecimento de tantos incidentes em sua rede quanto forem suas capacidades de detecção, ainda mais considerando que os ataques direcionados aumentam a cada ano.

De acordo com as pesquisas realizadas com as organizações da região, 70% consideram que o phishing se apresenta como um ataque com alta probabilidade de ocorrência, seguido pela infecção por códigos maliciosos (63%) e pelo roubo de credenciais de acesso (56%). Por outro lado, 30% dos profissionais afirmaram ter sofrido algum incidente de segurança nos últimos 12 meses.

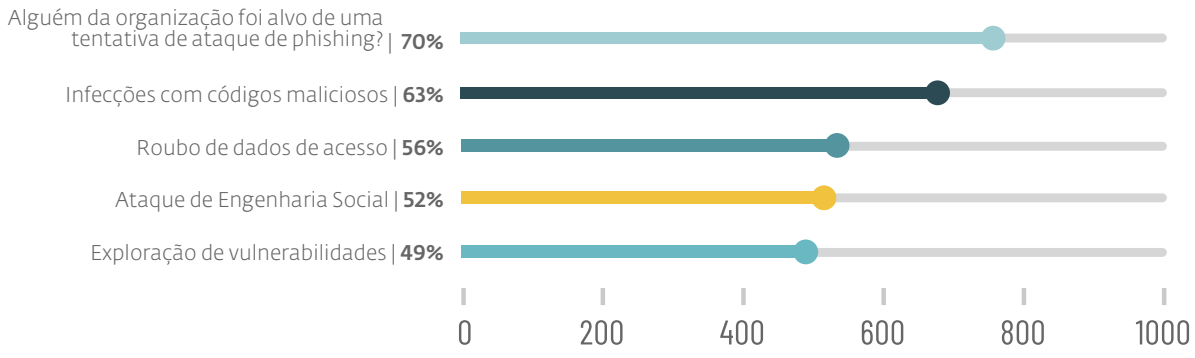

GRÁFICO 2. *NÚMEROS REVELADOS PELOS QUESTIONÁRIOS AO PERGUNTAR SOBRE OS TIPOS DE ATAQUES QUE AS ORGANIZAÇÕES SOFRERAM EM 2022.*

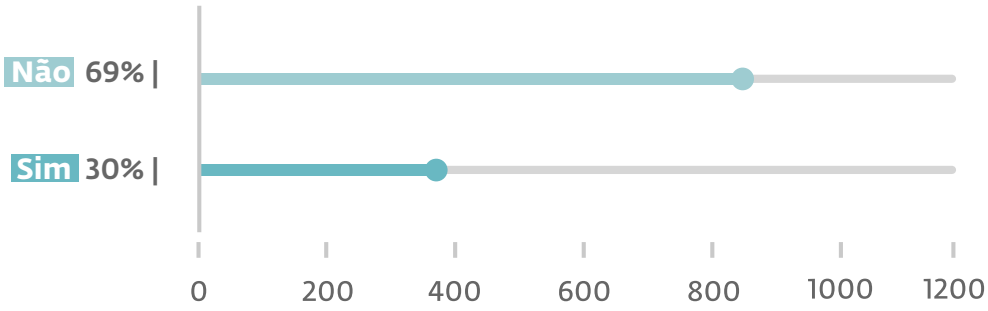

GRÁFICO 3. *USUÁRIOS QUE SOFRERAM INCIDENTES DE SEGURANÇA EM 2022*

Se analisarmos os dados dos questionários, metade afirmou não ter sofrido incidentes de segurança durante o último ano e afirmam possuir tecnologia suficiente para gerenciá-los. No entanto, se considerarmos que a quantidade de detecções maliciosas aumenta a cada ano, a interpretação pode ser que metade dos profissionais não reconheceu incidentes de segurança nos ativos de sua organização, independentemente de tê-los de fato sofrido ou não.

INCIDENTES NO BRASIL

Ao entender as principais ameaças cibernéticas e incidentes, as empresas estarão melhor preparadas para enfrentar os desafios que se apresentam no mundo digital em constante transformação. Baseado em dados coletados através da Telemetria da ESET, confira quais foram as ameaças que afetaram empresas e organizações no Brasil durante o ano de 2022.

AMEAÇAS A DISPOSITIVOS MOBILE CORPORATIVOS

O cenário corporativo tem passado por uma transformação digital acelerada, impulsionada pela crescente adoção de dispositivos mobile para fins profissionais. Smartphones e tablets tornaram-se ferramentas indispensáveis para o mundo dos negócios, proporcionando maior produtividade, mobilidade e comunicação instantânea entre funcionários e parceiros comerciais. Contudo, essa mobilidade também bre portas para uma nova gama de ameaças cibernéticas que visam os dispositivos mobile corporativos.

O sistema operacional Android, sendo amplamente utilizado e de código aberto, tornou-se um alvo atrativo para cibercriminosos que buscam explorar vulnerabilidades e obter acesso a informações sensíveis e confidenciais. A segurança dos dispositivos Android corporativos é de suma importância para garantir a integridade dos dados empresariais, a proteção de propriedade intelectual e a continuidade das operações.

COMO ESTAR PROTEGIDO?

- Atualizações e Patches: Mantenha os dispositivos Android atualizados com as versões mais recentes do sistema operacional e dos aplicativos. As atualizações e patches frequentes podem corrigir vulnerabilidades conhecidas.
- Gerenciamento de Dispositivos Móveis (MDM): Utilize soluções de Gerenciamento de Dispositivos Móveis para monitorar e controlar remotamente os dispositivos na rede da empresa. Isso permite implementar políticas de segurança, rastrear dispositivos perdidos ou roubados e aplicar restrições de uso.
- Restrições de Aplicativos: Limite a instalação de aplicativos apenas a lojas oficiais, como a Google Play Store. Desative a opção de instalação de aplicativos de fontes desconhecidas para evitar a instalação de apps falsos.
- Autenticação Forte: Exija autenticação forte para acessar dispositivos e aplicativos, como PINs, senhas, biometria ou autenticação em duas etapas

PHISHING

No cenário dinâmico e em constante evolução da cibersegurança, o phishing emergiu como uma das ameaças mais persistentes e enganosas enfrentadas por organizações em todo o mundo. Durante o ano de 2022, o ambiente empresarial continuou sendo um alvo atrativo para cibercriminosos que aprimoraram suas táticas e estratégias de ataque para explorar vulnerabilidades e enganar funcionários e executivos. Os casos de phishing direcionados a empresas se tornaram mais sofisticados e personalizados, visando explorar as fraquezas humanas e técnicas para obter acesso a informações confidenciais e sistemas críticos.

COMO ESTAR PROTEGIDO?

- Conscientização dos Funcionários: Eduque todos os funcionários sobre o que é o phishing, como identificar e relatar e-mails suspeitos e quais são as melhores práticas de segurança cibernética. A conscientização é a primeira linha de defesa.
- Simulações de Phishing: Realize simulações de phishing regulares para testar a capacidade dos funcionários de identificar e-mails falsos. Isso ajuda a reforçar o treinamento e identificar áreas de melhoria.
- Verificação de Remetentes: Instrua os funcionários a sempre verificar os remetentes dos e-mails antes de clicar em links ou baixar anexos. Desconfie de e-mails de remetentes desconhecidos ou endereços ligeiramente diferentes dos legítimos.
- Links e Anexos Suspeitos: Evite clicar em links ou baixar anexos de e-mails não solicitados, especialmente se solicitarem informações pessoais ou credenciais.
- Validação de Solicitações: Sempre que receber um e-mail solicitando informações confidenciais, verificação de conta ou pagamentos, verifique a autenticidade da solicitação pessoalmente ou por meio de canais oficiais da empresa.
- Habilitação de Autenticação em Duas Etapas (2FA): Implemente a autenticação em duas etapas em todas as contas e sistemas que permitem essa opção. Isso adiciona uma camada extra de segurança.

DOWNLOADERS E DROPPERS

No complexo cenário da cibersegurança, os cibercriminosos continuam desenvolvendo estratégias cada vez mais sofisticadas para comprometer a segurança de empresas e organizações. Entre as táticas que se destacam pela sua eficácia e capacidade de evasão das defesas cibernéticas, estão os Downloaders e Droppers. Essas ferramentas maliciosas têm sido utilizadas de forma crescente para facilitar a disseminação de malware e executar ataques altamente direcionados.

O termo "Downloader" refere-se a um tipo de malware projetado especificamente para baixar e instalar outros componentes maliciosos em sistemas comprometidos. Por outro lado, os "Droppers" são projetados para entregar e soltar esses componentes em um sistema, geralmente de forma furtiva e sem levantar suspeitas.

COMO ESTAR PROTEGIDO?

- Atualizações Regulares de Software: Mantenha todos os sistemas, aplicativos e software atualizados com os patches mais recentes. Isso ajuda a corrigir vulnerabilidades conhecidas que podem ser exploradas por Downloaders e Droppers.
- Firewalls e Filtros de Conteúdo: Utilize firewalls e filtros de conteúdo para monitorar e controlar o tráfego de rede, bloqueando o acesso a sites maliciosos e prevenindo downloads não autorizados.
- Solução de segurança atualizada: Use soluções antivírus e antimalware atualizadas em todos os dispositivos para detectar e bloquear downloaders e droppers antes que eles se infiltrem.
- Restrição de Permissões: Implemente políticas de restrição de permissões que limitem a execução de arquivos de locais não confiáveis ou desconhecidos.
- Filtragem de E-mails: Implemente filtros de e-mail para bloquear mensagens com anexos maliciosos ou links suspeitos.
- Verificação de Sites e Links: Utilize serviços de verificação de sites e links para determinar se um site é seguro antes de acessá-lo ou fazer o download de conteúdo.

RATS E WORMS

Entre essas ameaças que tiveram mais detecções estão os RATs (Remote Access Trojans, ou Trojans de Acesso Remoto) e Worms. Ambos são componentes-chave em ataques digitais sofisticados, capazes de causar danos significativos às operações e à segurança das organizações.

RATs são tipos específicos de malware projetados para fornecer aos atacantes um acesso remoto completo aos sistemas comprometidos. Esses trojans permitem que os cibercriminosos assumam o controle total dos dispositivos, explorando-os como pontos de entrada para infiltrar-se na rede corporativa e acessar informações confidenciais. Por outro lado, os Worms são malwares que se propagam de sistema para sistema, explorando vulnerabilidades e espalhando-se rapidamente, muitas vezes sem a necessidade de interação do usuário. Ao compreender a ameaça representada por RATs e Worms, as empresas podem adotar medidas de segurança proativas para mitigar riscos.

COMO ESTAR PROTEGIDO?

- Segurança em Camadas: Implemente uma abordagem de segurança em camadas, incluindo firewalls, antivírus, antimalware, IDS/IPS e soluções de proteção de endpoint.
- Controle de Acesso: Estabeleça políticas de controle de acesso para limitar os privilégios de usuários e sistemas somente ao necessário.
- Monitoramento de Rede: Implemente soluções de monitoramento de rede para detectar padrões suspeitos de tráfego que possam indicar a presença de RATs ou a propagação de Worms.
- Segmentação de Rede: Divida a rede em segmentos isolados, limitando a propagação de Worms e isolando partes críticas da infraestrutura.
- Análise de Comportamento: Use soluções de análise de comportamento para identificar atividades incomuns e padrões de execução de malwares.
- Testes de Penetração: Realize testes regulares de penetração para identificar vulnerabilidades em sua infraestrutura.

EXPLOITS

Entre as ameaças, os exploits se destacam como ferramentas de ataque poderosas, capazes de explorar vulnerabilidades em sistemas e aplicativos para comprometer a segurança de empresas e organizações. Esses exploits representam um risco significativo, permitindo que cibercriminosos se infiltrem em redes corporativas, expondo dados sensíveis e interrompendo operações críticas.

Exploits são códigos maliciosos desenvolvidos para explorar brechas em software desatualizado ou vulnerável. Quando bem-sucedidos, permitem que cibercriminosos obtenham acesso não autorizado a sistemas, executem comandos arbitrários e implantem malware. O uso de exploits pode variar de ataques direcionados a campanhas em larga escala, impac-

tando organizações de todos os tamanhos e setores.

Criminosos possuem duas principais formas de abordagem a um ambiente, a mais usada e que interage com pessoas é o phishing, já citado anteriormente, e a que pode permitir acesso ao ambiente sem nenhum tipo de interação com pessoas, utilizando explorações de vulnerabilidades para pavimentar o caminho até o comprometimento. Este tipo de abordagem é extremamente direcionado para uma aplicação e um sistema operacional específicos e, por explorarem comportamentos incomuns gerados por este conjunto de softwares as variações costumam não ocorrer tão frequentemente.

COMO ESTAR PROTEGIDO?

- Gestão de Software e Patches: Mantenha sistemas operacionais, aplicativos e software de segurança atualizados com os patches mais recentes para corrigir vulnerabilidades conhecidas.
- Segurança em Camadas: Implemente múltiplas camadas de segurança, incluindo firewalls, antivírus, antimalware, IDS/IPS e soluções de proteção de endpoint.
- Monitoramento de Vulnerabilidades: Utilize ferramentas de monitoramento de vulnerabilidades para identificar e corrigir falhas de segurança em tempo hábil.
- Avaliações de Segurança: Realize testes regulares de penetração e avaliações de segurança para identificar e corrigir vulnerabilidades antes que sejam exploradas.
- Filtragem de E-mails e Tráfego Web: Utilize soluções de filtragem para bloquear e-mails e tráfego da web que contenham exploits conhecidos.

RANSOMWARE

O ransomware não apenas compromete a segurança e a continuidade das operações corporativas, mas também coloca em risco a confidencialidade e a integridade dos dados empresariais. Há muito tempo o ransomware tem sido foco de muitas de nossas campanhas de conscientização tamanha importância e notoriedade que ele tem ganho no cenário de ameaças digitais ao longo do tempo no Brasil. Essa ameaça se mostrou como a mais eficiente em prover recursos financeiros para os cibercriminosos, permitindo que eles desenvolvam outras campanhas maliciosas para afetar outras pessoas e empresas, sejam essas campanhas de ransomware ou outros tipos de códigos maliciosos.

O ransomware é um tipo de malware projetado para criptografar os dados de uma vítima, tornando-os inacessíveis, e então exigir um resgate em troca da chave de descriptografia. Esses ataques deixam as organizações reféns das demandas dos criminosos, afetando operações, interrompendo negócios e, muitas vezes, resultando na perda irreparável de dados sensíveis.

COMO ESTAR PROTEGIDO?

- Backup Regular de Dados: Mantenha backups regulares e atualizados dos dados críticos. Armazene esses backups em locais isolados da rede, como mídias off-line, para evitar que também sejam criptografados.
- Atualizações de Software: Mantenha sistemas operacionais, aplicativos e softwares de segurança atualizados com os patches mais recentes. Isso ajuda a corrigir vulnerabilidades que podem ser exploradas por ransomware.
- Treinamento de Funcionários: Eduque os funcionários sobre os riscos do ransomware, incluindo a não abertura de anexos ou cliques em links suspeitos em e-mails.
- Filtragem de E-mails: Utilize soluções de filtragem de e-mails para bloquear mensagens maliciosas e anexos perigosos.
- Firewalls e Antivírus Atualizados: Implemente firewalls robustos e soluções antivírus atualizadas para identificar e bloquear atividades maliciosas.
- Restrição de Privilégios: Limitar os privilégios dos usuários, garantindo que apenas aqueles que precisam tenham acesso a áreas críticas da rede.
- Segmentação de Rede: Separe a rede em segmentos isolados para limitar a propagação do ransomware em caso de infecção.

CONCLUSÕES

O relatório que apresentamos sobre o cenário de segurança cibernética na América Latina e no Brasil em 2022 fornece uma visão dos desafios enfrentados pelas empresas e organizações em meio ao ambiente digital em rápida evolução. Ao analisarmos os dados coletados ao longo do ano, ficou evidente que as ameaças cibernéticas alcançaram um nível preocupante de sofisticação, colocando em xeque a proteção dos ativos digitais e a continuidade dos negócios.

No decorrer do ano, empresas de diversos setores enfrentaram uma diversidade de ataques, desde invasões de ransomware que paralisaram operações e exigiram resgates milionários, até vazamentos de dados que expuseram informações confidenciais de clientes e funcionários, causando danos irreparáveis à reputação das organizações.

Sem dúvidas, é necessário mais do que nunca investir em tecnologias e soluções de segurança de ponta. As defesas tradicionais muitas vezes se mostraram insuficientes diante das táticas cada vez mais avançadas dos cibercriminosos. A implementação de sistemas de segurança mais robustos, a utilização de inteligência artificial e aprendizado de máquina, e a constante atualização das políticas de segurança são fundamentais para proteger os ativos digitais das organizações.

Além disso, a conscientização dos colaboradores também se revela um pilar essencial na prevenção de ataques cibernéticos. A educação sobre as melhores práticas de segurança cibernética, a identificação de ameaças potenciais e a promoção de uma cultura de segurança digital são aspectos que devem ser priorizados por todas as empresas. A segurança cibernética não é apenas uma escolha, mas uma necessidade imperativa para o sucesso e a sustentabilidade das empresas no mundo digital em constante transformação.

SOBRE ESET

1 bilhão de usuários no mundo	**+ 7 mil** canais de vendas
+ 400 mil clientes corporativos	**+ 200** países com presença comercial

Digital Security
Progress. Protected.