Proteger o negócio do Super Bock Group

O aumento da dependência das operações de negócio dos sistemas de informação fez com que o grupo aumentasse a perceção de risco relacionadocom a exposição às ciberameaças.

A ideia foi criar um ponto de contacto único, disponível 24x7, para monitorizar e reagir a incidentes de segurança.

O Super Bock Group

A atividade principal do Super Bock Group (SBG) assenta no negócio das cervejas e das águas engarrafadas. É uma área extremamente competitiva na qual a concorrência, local ou internacional, é forte e muito ativa. O SBG procura ser diferenciador nestes mercados, tanto pelas suas marcas e produtos como pela sua agilidade e capacidade de ir ao encontro das necessidades dos seus clientes.

O SBG está ainda presente nos segmentos dos refrigerantes, dos vinhos, na produção e comercialização de malte e no negócio do turismo, detendo dois ativos de referência na região de Trás-os-Montes: os Parques Lúdico-Termais de Vidago e Pedras Salgadas.

A empresa é detida por capital maioritariamente português, 56% pelo Grupo VIACER e 44% pelo Grupo Carlsberg.

A transformação digital pode ser potenciadora da proximidade do grupo aos seus clientes, e um veículo de diferenciação na oferta ao mercado de bens de grande consumo. André Miranda, manager de arquitetura e projetos de TI no SBG, refere que "*os meios digitais de relacionamento entre as empresas, e destas com os consumidores dos seus produtos, podem ser fatores de diferenciação e potenciadores de crescimento, tanto do SBG como dos seus parceiros*".

Uma das características do negócio com a qual os sistemas de informação têm de lidar é a dispersão geográfica do negócio. A existência de vários centros de produção, plataformas logísticas ou de uma rede de distribuição dispersa no território nacional, ou em mercados externos, aumenta a capilaridade da atuação dos sistemas de informação. Nesse sentido, o caminho que tem vindo a ser seguido é "*o da centralização de sistemas, de forma a otimizar a reutilização da nossa infraestrutura e aplicações de negócio*", explica André Miranda.

O Super Bock Group em 2018

585 Milhões de litros produzidos

458 Milhões de euros em vendas

51 Milhões de euros de resultado líquido

1.310 Colaboradores

(Fonte: Relatório de gestão de 2018)

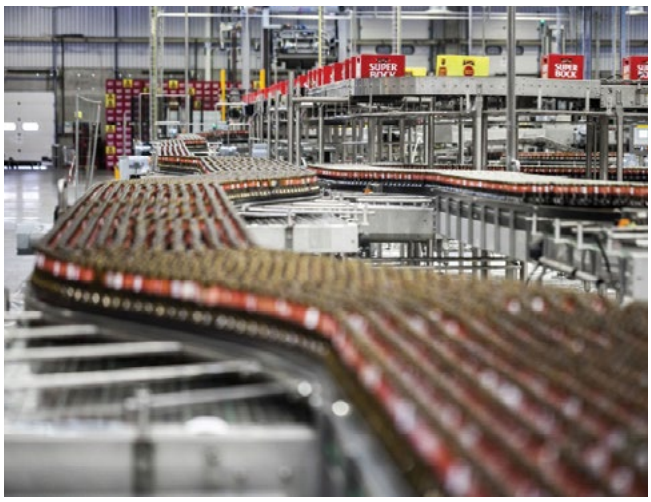
> *"Há cada vez mais incidentes sofisticados de tentativa de fraude. Estas situações complexas, e que normalmente envolvem engenharia social, são também analisadas pelo SOC."*
>
> **André Miranda**
> Manager | Arquitetura e projetos de TI
> **Super Bock Group**

A importância e relevância deste grupo industrial no panorama nacional, associado à digitalização e aumento da dependência dos sistemas de informação, fez com que houvesse um aumento da perceção de risco relacionado com a exposição às ciberameaças.

Os resultados das primeiras auditorias e análises de segurança fizeram com que o tema da cibersegurança entrasse para a agenda com duas opções óbvias. A primeira foi reconhecer a necessidade de criar um Security Operations Center (SOC), um ponto de contacto único, disponível 24x7, para monitorização e reação a incidentes de segurança. A segunda é que essas competências não deveriam estar dentro de portas.

A aposta foi recorrer a um serviço externo especializado capaz de acompanhar os incidentes em tempo real.
A escolha foi a Claranet.

> *"Temos uma visibilidade muito melhor dos incidentes de segurança da nossa infraestrutura e somos apoiados por uma equipa de especialistas."*
>
> **André Miranda**
> Manager | Arquitetura e projetos de TI
> **Super Bock Group**



claranet cyber security

Key services:

- Security Operations Center
- SOC as a Service
- Security Testing
- 24x7 Support
- Phishing & Social Engineering

Para mais informações sobre a oferta Claranet e seus benefícios consulte:
www.claranet.pt

Super Bock Group cria Security Operations Center

Ao começar a medição de ameaças de cibersegurança, o Super Bock Group concluiu que tinha uma média de 100 incidentes anuais.

Precisava da ajuda de um especialista para monitorizar e controlar em tempo real as ameaças e ser capaz de reagir rapidamente aos incidentes identificados.

O Super Bock Group (SBG) possui alguma exposição digital tanto por via das marcas como pela necessidade de disponibilizar várias aplicações para parceiros de negócio que acedem a estas através da internet. Por outro lado, tanto o SBG como os seus parceiros são altamente dependentes dos sistemas de informação para operar. Neste cenário, a disponibilidade dos sistemas é crítica para a normal continuidade do negócio. A grande digitalização dos processos internos da organização, tal como a crescente dependência da relação com os clientes dos meios digitais, fez com que a segurança dos sistemas de informação do grupo ganhasse relevância. André Miranda, manager de arquitetura e projetos de TI no SBG, aborda a importância do Security Operations Center (SOC) implementado e reconhece as melhorias alcançadas com os serviços prestados pela Claranet no domínio da cibersegurança.

Como entrou o tema da cibersegurança na agenda do Super Bock Group?

Os principais fatores para a crescente consciencialização dos stakeholders do grupo para o risco da cibersegurança nos últimos anos foi a realização de alguns processos de auditoria, que evidenciaram oportunidades de melhoria neste domínio.

Em média, sofrem quantos ataques por ano?

Temos uma baixa maturidade na contabilização de incidentes de cibersegurança, mas atualmente registamos cerca de 100 por ano. Cada um destes incidentes é processado por especialistas.

Que soluções ou ferramentas de gestão asseguravam até aqui as operações do Super Bock Group e quais eram as suas limitações?

Embora usássemos algumas ferramentas de auditoria, tínhamos uma abordagem interna e muito pontual à cibersegurança. Sentíamos falta de capacidade, tanto de conhecimento como de disponibilidade das equipas internas do SBG, para a cibersegurança. Fizemos algumas auditorias externas, tanto a nível técnico como processual, e concluímos que necessitávamos de endereçar a esta área um maior foco e dedicação.

O que originou a necessidade de o Super Bock Group recorrer a um serviço de Security Operations Center?

A vantagem de recorrermos a um serviço de SOC é a monitorização ativa da nossa infraestrutura e aplicações, mantendo a orientação dos sistemas de informação para o desenvolvimento de aplicações e as áreas onde consideramos que podemos trazer mais valor para o negócio do SBG.

No que consiste a solução implementada pela Claranet?

Não se trata especificamente de uma solução, mas sim de um roadmap plurianual de atividades relacionadas com cibersegurança, em que se enquadra a adoção de um SOC. Além desta adoção temos outras atividades que visam a realização de testes regulares, tanto técnicos como comportamentais, e também ações de sensibilização e formação dos utilizadores finais. No nosso entendimento, a abordagem à cibersegurança deve tentar ser holística.

De ano para ano aumenta a frequência de ataques? As ameaças são cada vez mais complexas e difíceis de detetar?

Temo-nos apercebido de que há cada vez mais incidentes sofisticados de tentativa de fraude. Estas situações complexas, e que normalmente envolvem engenharia social, são também analisadas pelo SOC. No entanto, é um caminho que estamos a começar a percorrer.

• • •

A solução implementada pela Claranet já permitiu detetar ameaças ao Super Bock Group que sem ela não seria possível, ou seria muito difícil, detetarem?

Sim. Temos evidências de situações de exposição a risco, que não teríamos detetado antes de termos o serviço de Managed Security Services. Na nossa experiência, estas situações não se materializaram em custos ou perdas de negócio para o SBG.

Tiveram recentemente um episódio de phishing? Que constrangimentos trouxe e como foi neutralizado?

Episódios de phishing têm ocorrido, mas os utilizadores já estão bastante sensibilizados para o tema e percebemos que o comportamento habitualmente é o correto.

As situações mais preocupantes hoje em dia são de spearphishing, por vezes associadas a engenharia social e combinadas com domain squatting. Estes ataques mais sofisticados, que envolvem múltiplas técnicas e vetores de ataque durante longos períodos de tempo, são complexos e requerem que as organizações também se preparem atempadamente e em múltiplas camadas, desde a monitorização ativa, oferecida por um SOC, passando pela robustez dos seus processos e pela formação e sensibilização dos utilizadores.

É também importante encararmos a cibersegurança como algo que extravasa a organização e que inclui os seus parceiros de negócio, uma vez que o risco pode vir destes.

Como chegam até esta solução e à Claranet como fornecedor/integrador?

Quando iniciámos o processo de pesquisa no mercado de soluções de Managed Security Services já conhecíamos a oferta da Claranet neste setor. Pareceu-nos apropriado, face ao diagnóstico que fizemos, a adoção do serviço de SOC de forma externalizada.

Quanto tempo demorou o processo de implementação?

O início do serviço foi feito aproximadamente em três semanas. O processo de afinação posterior demorou cerca de três meses, mas há sempre um ajuste continuado a realizar. Neste momento estamos a chegar ao ponto de estabilidade e com o serviço em "velocidade cruzeiro".

Como foi a experiência com a Claranet no processo de onboarding?

Desde cedo no processo percebemos que a Claranet tinha experiência no onboarding de clientes, pelo processo estruturado que utilizou para a preparação do serviço para o Super Bock Group. Embora o serviço tenha muitos pontos de contacto com o que já realizavam para outras empresas, houve uma fase de conhecimento mútuo, importante para que o serviço tenha sido ajustado à realidade da nossa empresa e do nosso negócio. Considero que houve aprendizagem de parte a parte neste processo.

Que procedimentos e precauções adotaram na concretização deste projeto?

O Super Bock Group lida na gestão dos seus sistemas de informação com vários parceiros externos. O principal ponto de cuidado na introdução da componente de Managed Security Services foi a integração dos novos processos com os processos de suporte existentes, e a articulação entre as várias entidades para que o dia a dia do serviço de cibersegurança decorra da melhor forma possível.

O projecto já está concluído? Que vantagens trouxe para os processos de negócio da empresa?

O projeto está concluído, mas temos consciência de que durante todo o tempo de prestação do serviço continuaremos a necessitar de fazer afinações. O serviço de SOC deve atuar como elevador transversal do nível de segurança dos processos de negócio.

Na perspetiva de segurança de informação, o que mudou com a introdução dos serviços do SOC?

Temos uma visibilidade muito melhor dos incidentes de segurança da nossa infraestrutura e somos apoiados por uma equipa de especialistas. Passamos também a ter uma capacidade melhorada de relatório de cibersegurança, tanto a nível operacional como de gestão.

Quais as áreas de negócio que obtiveram maiores benefícios com este projeto?

Um projeto de cibersegurança deve ser encarado pela organização como transversal. Todas as áreas de negócio são clientes e altamente dependentes dos sistemas de informação, pelo que devem encarar os riscos de cibersegurança como algo inerente a uma realidade de negócio cada vez mais digital.

Que melhorias estão previstas introduzir num futuro próximo?

O nosso plano de cibersegurança foi enriquecido com a inclusão dos Managed Security Services, mas temos outras iniciativas planeadas para o futuro, centradas na sensibilização dos colaboradores e na proteção da nossa infraestrutura. Não encaramos a cibersegurança como uma corrida com uma meta a atingir, mas sim como um treino continuado que faz com que o Super Bock Group esteja cada dia mais capaz.

Para mais informações sobre a oferta Claranet e seus benefícios consulte: www.claranet.pt