POLITÉCNICO DE LEIRIA

BOAS PRÁTICAS DE CIBERSEGURANÇA

NAS EMPRESAS DO SETOR AGROINDUSTRIAL

S4agro Soluções sustentáveis para o setor agroindustrial

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu de Desenvolvimento Regional

SOBRE O PROJETO S4AGRO

O projeto S4AGRO tem como objetivo principal a qualificação das PME do setor agroindustrial, no sentido de se capacitarem para a adoção de soluções inovadoras e sustentáveis. Os benefícios esperados são o aumento da produtividade, da eficácia e da eficiência, no contexto da indústria 4.0 e da economia circular.

A digitalização das empresas, inerente à implementação deste projeto, implica necessariamente a adoção de boas práticas de cibersegurança nas empresas. Para tal, foi realizado um estudo junto de PME, baseado no Quadro Nacional de Referência para a Cibersegurança do Centro Nacional de Cibersegurança (CNCS), no sentido de identificar fatores críticos para a segurança dos seus sistemas informáticos, ccom vista à qualificação das PME e à aplicação de boas práticas neste domínio. Do estudo realizado na Atividade 4 do projeto, resultou o Manual de Boas Práticas em Cibersegurança que se encontra resumido neste documento..

BOAS PRÁTICAS DE CIBERSEGURANÇA NAS EMPRESAS DO SETOR AGROINDUSTRIAL

ESTABELECER OS NORMATIVOS BASILARES DE CIBERSEGURANÇA

Devem ser estabelecidos normativos formais, escritos, que tenham a aprovação da gestão de topo, com o objetivo de regularem a segurança de informação e cibersegurança. Este corpo normativo deve, no mínimo, contemplar os requisitos básicos de segurança da informação na organização. Deve, igualmente, ser redigido numa linguagem acessível, tendo em conta que essa documentação será dada a conhecer a todos os colaboradores.

DEFINIR OS RESPONSÁVEIS PELA SEGURANÇA DA INFORMAÇÃO E SUAS RESPETIVAS FUNÇÕES

Apesar de as empresas identificarem genericamente os responsáveis internos, de acordo com critérios de necessidade operacional, raramente se consideram as responsabilidades internas, enquadráveis no domínio da cibersegurança. A nomeação de responsáveis no domínio da informática e da cibersegurança deve ser tida em conta, nomeadamente no que diz respeito à manutenção da infraestrutura de IT/OT, à gestão de inventários e gestão de riscos.

ESTABELECER OS FUNDAMENTOS PARA PRÁTICAS DE SEGURANÇA BASEADAS EM ANÁLISE DE RISCO

É importante fomentar uma cultura de cibersegurança nas empresas, que assente em princípios, mesmo que simplificados, de gestão de risco. Um exemplo de simplificação é a concentração dos esforços de gestão de risco nos ativos considerados mais críticos, quer estes sejam processos, equipamentos ou instalações.

Deverá estabelecer-se um plano de tratamento de riscos, que esteja concentrado nos riscos considerados mais elevados ou com impactos mais onerosos. Este plano deve ter por objetivo mitigar os riscos de segurança selecionados, reduzindo-os a um nível que seja considerado aceitável para a organização.

IMPLEMENTAR CAPACIDADES MÍNIMAS DE MONITORIZAÇÃO DE SEGURANÇA

A monitorização permite que as empresas tenham uma visão abrangente sobre o que se passa na sua organização ao nível da sua segurança. Uma boa capacidade de monitorização é essencial para a recolha de informação crítica, cuja análise possa contribuir para determinar ações de mitigação e níveis de proteção eficazes.

É importante que as empresas do setor agroindustrial disponham de uma capacidade de monitorização que inclua informação de registos de auditoria (logging) dos seus sistemas, quer informáticos quer industriais, pelo menos dos mais críticos, com um grau de detalhe que contemple as seguintes informações:

- Identificação do utilizador;
- Tipo de evento;
- Data, hora e fuso horário;
- Indicação de sucesso ou falha;
- Origem do evento;
- Identificação ou nome dos dados, componentes de sistemas ou recursos afetados.

Esta informação permitirá não só detetar ataques, mas também proceder ao diagnóstico de causas de problemas.

Deverão ser consideradas as obrigações legais quanto ao cumprimento do Regulamento Geral de Proteção de Dados (RGPD).

GARANTIR A EXISTÊNCIA DE BACKUPS ÍNTEGROS

Os ataques de ransomware, podem ter o seu impacto reduzido através de práticas eficientes e eficazes de backups, permitindo a recuperação da totalidade ou quase totalidade da informação afetada pelo malware. Aconselhando-se:

- Adicionar aos backups as configurações dos sistemas críticos;
- Automatizar os sistemas de backup e recuperação, garantindo eficiência e consistência do seu funcionamento;
- Separar o armazenamento dos backups da rede corporativa, protegendo-os de ameaças à rede interna;
- Executar testes regulares de recuperação, no sentido de garantir a qualidade e integridade dos backups;
- Duplicar os backups críticos para uma localização distinta.

PROTEGER CONFIGURAÇÕES DE SISTEMAS, REDES E EQUIPAMENTOS

A identificação de medidas protetivas das configurações dos equipamentos, sistemas e redes ajuda a proteger adequadamente as organizações. Destacam-se aqui as seguintes prioridades:

- Controlo do acesso à Internet através, por exemplo, da configuração de um proxy, limitando a exposição dos sistemas internos aos perigos da Internet e facilitando a aplicação de medidas restritivas de acesso;
- Aumentar a robustez das configurações de sistemas e redes, eliminando configurações e acessos por omissão, desativando os serviços desnecessários, e maximizando a segurança dos serviços indispensáveis;
- Implementação de sistemas de segurança ao nível dos dispositivos terminais, instalando, nomeadamente, antivírus e sistemas de deteção de intrusões;
- Instalação de sensores em dispositivos de sistemas industriais antigos para deteção reforçada de incidentes ou eventos anómalos;
- Definição e aplicação de uma política de Bring Your Own Device (BYOD) que garanta a aplicação de restrições a tais dispositivos, com o intuito de proteger a rede interna.

DETETAR E MITIGAR VULNERABILIDADES NOS SISTEMAS

As organizações do setor devem assumir uma postura mais proativa no domínio da deteção e mitigação de vulnerabilidades.

A deteção, através da realização de scans periódicos à rede, destina-se a detetar fragilidades próprias dos sistemas e redes da organização, antes mesmo da existência de soluções ou atualizações de segurança. Isso permitirá mitigar ataques em janelas temporais que medeiam o conhecimento de tal vulnerabilidade e a disponibilização de uma atualização por parte do fabricante.

A mitigação consiste em resolver ou mitigar a exposição de segurança resultante da vulnerabilidade detetada. A resolução pode conseguir-se no caso de já haver uma atualização. Se não for o caso, a mitigação terá de passar por procedimentos alternativos ou até algumas restrições de funcionalidades para evitar impactos maiores resultantes de incidentes.

PLANEAR CONTINUIDADE DE NEGÓCIO E RECUPERAÇÃO DE DESASTRES

Embora seja frequente as empresas de maior dimensão disporem de um Plano de Continuidade de Negócio e Recuperação de Desastres, raros são os planos que preveem contingências relativas à cibersegurança.

É crucial que as empresas tenham em conta a continuidade de negócio dos sistemas de informação e dos sistemas industriais na sequência de incidentes de segurança. O plano de continuidade de negócio deverá contemplar os ativos críticos.

É de igual importância, que sejam realizados testes periódicos ao plano de continuidade de negócio estabelecido.

PREPARAR ADEQUADAMENTE UMA CAPACIDADE DE RESPOSTA

Os ciberataques provocados por ransomware e outros tipos de softwares maliciosos podem dar origem a incidentes que afetaram a confidencialidade, integridade e/ou disponibilidade de informação) podendo implicar danos avultados para a organização.

A resposta atempada a incidentes de segurança é primordial no sentido de mitigar o impacto dos incidentes de segurança e assegurar a conformidade com requisitos legais ou regulatórios, como seja o Regulamento Geral de Proteção de Dados (RGPD). Sendo uma função que pressupõe conhecimentos especializados, é aconselhável a sua subcontratação num quadro de prestação de serviços de segurança.

CONTROLAR ADEQUADAMENTE A SEGURANÇA DA CADEIA LOGÍSTICA

Existe uma dependência do setor agroindustrial junto de fornecedores externos na intervenção em equipamentos industriais e informáticos.
As empresas do setor devem tomar providências, em sede contratual, junto dos seus fornecedores no sentido de assegurar:

- Cláusulas de confidencialidade;
- Restrições no acesso de subcontratados à informação da empresa;
- Aspetos de continuidade de negócio, assegurando o fornecimento regular de atualizações de segurança;
- Requisitos de notificação de incidentes, com definição de níveis de serviços relativos a tempos de resposta;
- Restrições específicas de segurança na subcontratação por parte da própria empresa subcontratada.

DEFINIR E EXECUTAR UM PLANO DE AUDITORIAS À SEGURANÇA

As empresas do setor agroindustrial devem estabelecer um plano de auditorias regulares, com a abrangência adequada aos sistemas considerados críticos.

Os testes, definidos neste plano, devem incluir os sistemas afetos a recursos industriais, assim como abranger as redes onde se encontram equipamentos contendo hardware ou software antigo, que não pode ser atualizado, no sentido de apurar se as camadas de segurança que os protegem são eficazes.

As auditorias não devem incidir apenas sobre a componente técnica, mas também sobre a componente comportamental, processual e política.

ASSEGURAR FORMAÇÃO ADEQUADA DOS COLABORADORES

A formação e consciencialização para as práticas de segurança informática por parte dos colaboradores de empresas do setor agroindustrial é reduzida.

Qualquer colaborador que tenha acesso a um computador com sistema de e-mail ou acesso à web poderá, através de práticas negligentes, infetar toda a rede interna da organização com software malicioso. Esta infeção poderá significar perdas avultadas para a empresa, resultantes em perdas de produtividade ou de reputação, e pagamento de multas ou indemnizações. Deve ser ministrada aos colaboradores uma formação mínima no domínio de práticas básicas de segurança da informação e comportamento defensivo em rede.

GERIR MUDANÇAS E ATUALIZAÇÕES NOS SISTEMAS

Muitos incidentes ocorrem por falta da aplicação atempada de atualizações dos softwares. Deve ser implementado um sistema de atualizações de segurança de sistemas, que garanta que estes se mantêm seguros.

O sistema de atualizações deve ser o mais eficiente possível, por forma a reduzir ao mínimo a janela temporal durante a qual os sistemas se mantêm vulneráveis. É importante ainda considerar que qualquer sistema informático ligado, ainda que por via indireta, a um sistema industrial, é um sistema prioritário para atualização, uma vez que poderá constituir uma via de acesso a funções críticas do negócio.

Devem ser mantidos registos de atualizações, com prioridade para as dos sistemas mais críticos. Idealmente, as atualizações deverão ser previamente testadas em ambientes próprios para esse efeito e só depois serem aplicadas aos sistemas em produção, no sentido de precaver eventuais falhas de compatibilidade que poderão resultar em perdas de produtividade.

DEFINIR E IMPLEMENTAR UMA ARQUITETURA DE SEGURANÇA

O conceito de arquitetura de segurança pode parecer complexo para as PME do setor agroindustrial, mas é possível implementá-lo numa perspetiva bastante prática, nomeadamente:

- Planeando a segmentação da rede interna, através da separação de ambientes informáticos de diferentes funções. Por exemplo, efetuando a separação entre as redes industrial, administrativa e a de servidores;
- Defendendo o perímetro de rede, quando se justifique e na medida do valor dos ativos protegidos;
- Instalando ferramentas anti-malware em todos os computadores pessoais, telemóveis, tablets, e outros equipamentos conectáveis;
- Aplicando segurança física, que restrinja o acesso de pessoas à proximidade de ativos críticos;
- Definindo um controlo de acessos, que identifique os utilizadores e o perfil ao qual devem pertencer, assegurando que esse perfil apenas tenha acesso à informação necessária para o desempenho da função.

FORTALECER CONTROLOS DE ACESSOS NOS DISPOSITIVOS DE INFORMÁTICOS E EM SISTEMAS INDUSTRIAIS

É comum as PME do setor agroindustrial recorrerem à subcontratação de serviços de manutenção para os seus sistemas informáticos e/ou industriais, pelo que o controlo de acessos adquire particular relevo.

O reforço das medidas de controlo de acessos a sistemas críticos (informáticos e industriais) é assim premente e deve ter em conta utilizadores internos e externos, bem como perfis de administração.

Algumas tecnologias que poderão ser utilizadas são: instalação de acessos através de redes privadas (VPN), sistemas de múltiplo fator de autenticação (MFA); restrição de acesso a certas redes internas; correta gestão de passwords; eliminação de contas de grupo; atribuição exclusiva de privilégios de administração a quem deles efetivamente necessite; imposição de controlos de acesso físico, com registo de entrada, e restrição de acessos a zonas onde se encontrem ativos críticos informáticos ou industriais vitais ao negócio.

CRIAR/COMPLEMENTAR O INVENTÁRIO DE ATIVOS/FUNÇÕES

A inventariação de ativos é um requisito basilar para assegurar uma melhor proteção ao nível da cibersegurança. É comum existirem ativos que não fazem parte de nenhum inventário da organização, ou que a sua existência não seja do conhecimento da equipa que faz a gestão da cibersegurança. Torna-se assim impossível aplicar medidas protetoras sobre esses ativos, potenciando as ameaças à organização.

Um inventário deve ser preciso e continuamente atualizado, assegurando dessa forma uma atempada e correta atuação em caso de ocorrências de incidentes de segurança. Esse grau de precisão e nível de atualização é vital nos ativos críticos da organização, nomeadamente equipamentos informáticos, de rede e sistemas industriais, permitindo facilitar a manutenção preditiva desses ativos bem como dos processos internos em que eles estejam envolvidos.

O Manual de Boas Práticas está disponível para consulta no website do projecto em www.s4agro.pt. Este manual faz parte da Atividade 4 (www.s4agro.pt/atividades/#atividade-4), desenvolvida pelo Instituto Politécnico de Leiria (ipleiria@ipleiria.pt).

Para conhecer melhor o projeto S4agro consulte o link www.s4agro.pt e acompanhe as ações do projeto através do Facebook em www.facebook.com/S4agro e do Linkedin: em www.linkedin.com/company/s4agro-soluções-sustentáveis-para-o-setor-agroindustrial/

Para mais informações acerca do projeto, contacte-nos por email: geral@s4agro.pt

S4agro

Soluções sustentáveis
para o setor agroindustrial

Promotor

Universidade da Beira Interior

Universidade de Évora

MED

Copromotores

i2a Politécnico de Coimbra

Politécnico de Leiria

IPG Instituto Politécnico da Guarda

Instituto Politécnico de Viana do Castelo

desde 2009 INOVCLUSTER Associação do Cluster Agro-industrial do Centro

Cofinanciado por:

COMPETE 2020

PORTUGAL 2020

UNIÃO EUROPEIA
Fundo Europeu
de Desenvolvimento Regional