Plano de continuidade da atividade

Um plano de continuidade da atividade oferece a uma empresa a oportunidade de planear a sua capacidade de continuar a fornecer produtos e serviços em prazos aceitáveis, e com uma capacidade predefinida durante uma crise. O plano irá apoiar os objetivos estratégicos, proteger a reputação e a credibilidade, e permitir que se mantenha resiliente face a um ciberataque.

O desenvolvimento deste plano irá ajudá-lo a antecipar-se à ameaça. Acredite quando lhe dizermos que não querer saber como reagir durante um incidente. O tempo de resposta é fundamental para minimizar os danos.

Para desenvolver o seu Plano de continuidade da atividade, deve elaborar o seguinte:

1. Ficha de trabalho de definição de prioridades: uma ferramenta que lhe permite inventariar os dados e as informações mais importantes para o êxito da sua organização. A definição da prioridade do que é mais importante proteger irá ajudá-lo a criar políticas eficazes e a tomar decisões de investimento inteligentes.

2. Plano de resposta a incidentes: Um plano abrangente e gradual para responder, corrigir e aprender rapidamente com cada incidente.

A ferramenta de atualização de software e a política de cópia de segurança dos dados também são fatores chave que contribuem para a sua resiliência global.

Existem outros recursos incluídos mais adiante no plano que o vão ajudar a reforçar a sua cibersegurança e resiliência, à medida que continua a melhorar o planeamento da continuidade da atividades da sua organização.

Ficha de trabalho de definição de prioridades

É chegado o momento de pensar nos dados, no software e no hardware mais importantes para o êxito da sua organização. A definição da prioridade do que é mais importante proteger irá ajudá-lo a criar políticas eficazes e a tomar decisões de investimento inteligentes.

Indique os dados mais importantes para o êxito da sua organização (números de cartões de crédito dos clientes, informações pessoais dos colaboradores, dados financeiros, etc.)

Indique o software mais importante para o êxito da sua organização (Office 365, MacOS, LINUX, etc.)

Indique as ferramentas de hardware e de software mais importantes para o funcionamento da sua organização (dispositivos móveis, portáteis, impressoras, scanners, etc.)

Identifique os 3 a 5 elementos das 3 listas precedentes que causariam mais danos à sua empresa se fossem perdidos, roubados ou não estivessem disponíveis.

Plano de resposta a incidentes (IRP)

Estabelecer práticas e políticas de prontidão cibernética ajuda a reduzir o risco, mas é importante assumir que a nossa empresa irá provavelmente enfrentar a qualquer momento um incidente de segurança que poderá ter impacto nas operações empresariais. Tentar determinar como responder durante um incidente não é boa ideia. O tempo de resposta é fundamental para minimizar os danos. Dispor de um plano bem definido pode fazer a diferença entre um incidente e uma catástrofe.

Um IRP abrangente e gradual permite responder, corrigir e aprender rapidamente com cada incidente. Este IRP funciona como um roteiro para o que fazer durante a resposta a um incidente de cibersegurança, o que assegura uma resposta estratégica e não apenas uma resposta reativa.

A nossa resposta a incidentes inclui três elementos principais:

1. **Preparar** para um possível incidente no futuro
2. **Responder** durante o incidente
3. **Recuperar** do incidente

Preparar

Diretrizes organizacionais:

O investimento que fizer na preparação trará muitos dividendos. Existem alguns elementos de resposta essenciais que devem ser realizados o mais brevemente possível para se preparar para os danos causados por um ataque e os reduzir. O CRI irá analisar e confirmar que incluiu o seguinte no seu Manual de procedimentos final.

1. **Nomear o líder de cibersegurança.** A nomeação de um líder de cibersegurança é essencial para a prontidão cibernética da sua empresa. O Líder de cibersegurança será responsável pela partilha de informações de prontidão cibernética com a sua força de trabalho e pela gestão do desenvolvimento das suas políticas de prontidão cibernética.

Medidas implementadas	Data de conclusão

2. **Implementar Políticas de 4 principais problemas de cibersegurança:** assegure que as políticas cibernéticas são definidas e partilhadas com os colaboradores que cumpram ou vão mais além dos requisitos do CRI.

Medidas implementadas	Data de conclusão

3. **Faça cópias de segurança dos dados e certifique-se de que consegue voltar a instalar os dados a partir das cópias de segurança.** A recuperação de um ataque será muito mais rápida e afetará muito menos as operações se tiver cópias de segurança atualizadas do software do sistema, das aplicações e, sobretudo, dos dados importantes. Também deverá assegurar que todas as pessoas na sua organização têm cópias de segurança, caso este processo não esteja centralizado. É importante testar regularmente as suas cópias de segurança.

Medidas implementadas	Data de conclusão

4. **Dê formação à sua força de trabalho.** Todos os membros da equipa devem conseguir identificar atividades suspeitas e saber quem contactar nesta eventualidade. Os colaboradores essenciais também deverão estar cientes do seu papel na resposta a um incidente.

Medidas implementadas	Data de conclusão

5. Estabelecer contactos. Estabeleça contactos internos e externos aos quais poderá recorrer se um incidente cibernético superar a sua capacidade de controlo.

Contacto para emergência de TI	[Indique aqui]
Fornecedor de serviços Internet	[Indique aqui]
Contacto para emergência jurídica	[Indique aqui]
Contacto para comunicações de emergência	[Indique aqui]

Responder

Algo de estranho está a acontecer com o computador de um colaborador, que não sabe o que fazer. Esta situação equivale a sentir o cheiro de fumo ou a ver uma pequena chama na sala do café.

O que deve fazer:

1. **Isole o problema**: retire imediatamente o dispositivo da rede
2. **Identifique o tipo de incidente** e tome a seguinte medida:

- ✓ Malware: retire imediatamente o dispositivo da rede
- ✓ Roubo de credenciais – desative mas não elimine a conta e redefinia a palavra-passe
- ✓ Violação de dados – ligue para o contacto de emergência de TI

- ✓ Ransomware: retire imediatamente o dispositivo da rede
- ✓ Ataque Denial of Service: contacte o gestor de TI e/ou a pessoa de contacto de suporte técnico externo

3. Determine o âmbito do incidente ao colocar estas perguntas:
   - ✓ Quando é que o incidente ocorreu?
   - ✓ Quem sofreu o impacto?
   - ✓ Qual é a natureza técnica do incidente? Como é que ocorreu? Temos conhecimentos internos para o resolver?
   - ✓ Quem está a par do incidente?
   - ✓ Ainda está a decorrer?

4. **Determine se pode ser controlado internamente** de forma adequada ou se precisa de contactar o suporte de TI externo para assegurar que a falha de segurança é resolvida de forma adequada.
5. **Continue a avaliar se o problema volta a ocorrer.** Caso seja pouco claro se o problema foi resolvido, peque por excesso e contacte um especialista para obter suporte.

Faça um resumo da forma como planeia isolar, identificar e determinar o âmbito de um incidente.

Recuperar

A crise passou e chegou o momento de as coisas voltarem ao normal. O âmbito do incidente e a gravidade do impacto determinarão quanto tempo e esforço serão necessários para a recuperação. No entanto, os passos básicos são os mesmos.

O que deve fazer.

1. Notifique todas as partes afetadas
2. Reponha o ID de utilizador e a palavra-passe do dispositivo comprometido
3. Aplique correções a todos os dispositivos
4. Volte a instalar o software e os dados a partir das cópias de segurança conforme necessário

Forneça abaixo um resumo da sua política e do plano de recuperação de um incidente para análise.

Recursos adicionais para a continuidade da atividade

À medida que continua a evoluir como organização, e a melhorar a sua cibersegurança e a resiliência, queremos fornecer-lhe duas ferramentas adicionais:

1. Árvore de decisão do plano de continuidade da atividade: ferramenta para orientá-lo nas principais decisões para fazer face a um incidente. Estão disponíveis espaços em branco para assegurar que está preparado.
2. Manual de procedimentos em caso de ransomware: Este guia tem como objetivo fornecer um roteiro para as empresas (por exemplo, pequenas e médias empresas, governos estaduais e locais) se protegerem contra esta ameaça crescente.